VMware vSphere: Optimize and Scale

Lab Manual

ESXi 7 and vCenter Server 7

VMware® Education Services
VMware, Inc.
www.vmware.com/education

VMware vSphere:
Optimize and Scale
Lab Manual
ESXi 7 and vCenter Server 7
Part Number EDU-EN-VSOS67-LAB (4/2020)

www.vmware.com/education

Typographical Conventions

The following typographical conventions are used in this course.

Conventions	Usage and Examples
`Monospace`	Identifies command names, command options, parameters, code fragments, error messages, filenames, folder names, directory names, and path names: • Run the `esxtop` command. • … found in the `var/log/messages` file.
`Monospace Bold`	Identifies user inputs: • Enter **`ipconfig /release`**.
Boldface	Identifies user interface controls: • Click the **Configuration** tab.
Italic	Identifies book titles: • *vSphere Virtual Machine Administration*
< >	Indicates placeholder variables: • <ESXi_host_name> • … the `Settings/<Your_Name>.txt` file

Contents

Lab 1 Accessing the Lab Environment

Objective and Tasks

Access the lab environment and verify that vSphere licenses are valid:

1. Access Your Lab Environment
2. Verify That the vSphere Licenses Are Valid
3. (Optional) Assign Valid vSphere Licenses
4. Add ESXi Hosts to vCenter Server

Task 1: Access Your Lab Environment

You use a View desktop or Remote Desktop connection to connect to your lab environment and you use the vSphere Client from the Student-A-01 desktop.

1. Use the information that is provided by your instructor to log in to your lab environment.
2. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**

3. Log in to the vSphere Client on Site B.
    a. In a new Firefox web browser tab, click **vSphere Site-B** on the bookmarks toolbar.
    b. Select **vSphere Client (SB-VCSA-01)**.
    c. On the login page, enter the vCenter Server lab credentials.

        User name: **`administrator@vsphere.local`**
        Password: **`VMware1!`**

        You can keep this tab open for future use in this lab.

Task 2: Verify That the vSphere Licenses Are Valid

You verify that the licenses for the vCenter Server systems and the ESXi hosts are valid for both Site A and Site B.

1. Verify that the licenses for the vCenter Server systems (Site A and Site B) are not expired.
    a. In the left pane, select **Host and Clusters**.
    b. Select **sa-vcsa-01.vclass.local**.
    c. In the right pane, click the **Configure** tab and click **Licensing** under System Settings.
    d. Verify that the license expiration date for the vCenter Server instance is not expired.
    e. Repeat the steps above to ensure that licensing is up to date on **sb-vcsa-01.vclass.local**.
2. Verify that the licenses for the ESXi hosts are valid (both Site A and Site B).
    a. In the left pane, expand the inventory until you see the ESXi hosts.
    b. Select **sa-esxi-04.vclass.local**.
    c. In the right pane, click the **Configure** tab and click **Licensing** under System Settings.
    d. Verify that the license for host sa-esxi-04.vclass.local is not expired.
    e. Repeat this step for the remaining ESXi hosts in the inventory (both Site A and Site B).
3. If the licenses are valid, jump to task 4. If any license has expired, see your instructor.

Task 3: (Optional) Assign Valid vSphere Licenses

You assign valid licenses to these vSphere components if the vCenter Server and ESXi host licenses are expired.

1. Select **Menu > Administration**.
2. Assign a vCenter Server license key to the vCenter Server instance.
   a. In the Navigator pane, select **Licenses**.
   b. In the Content pane, click the **Licenses** tab.
   c. Click **+Add New Licenses**.
   d. On the Enter license keys page, enter the vCenter Server and vSphere Enterprise Plus license keys provided by your instructor in the **License keys** text box.

      You must enter the license keys on separate lines.
   e. Verify that both licenses are listed correctly in the text box and click **Next**.
   f. On the Edit license names page, enter **`VMware vCenter Server`** and **`VMware vSphere ESXi`** in the appropriate **License name** text boxes and click **Next.**
   g. On the Ready to complete page, click **Finish**.
   h. In the Licenses pane, click the **Assets** tab.
   i. Select the vCenter Server **sa-vcsa-01.vclass.local** check box and click **Assign License**.
   j. Select the vCenter Server license and click **OK**.
   k. Repeat this step to apply the proper license for vCenter Server sb-vcsa-01.vclass.local.
3. Assign the vSphere Enterprise Plus license key to the ESXi hosts for Site A and Site B.
   a. In the center pane, click the **Hosts** tab.
   b. Select all hosts by selecting the check box to the left of the Asset column header.
   c. Click **Assign License** and click **Yes** to perform the action on host objects.
   d. In the Assign License dialog box, select the vSphere Enterprise Plus license key and click **OK**.
   e. Repeat this step and ensure that licensing is applied to any other ESXi hosts (in Site A or Site B).

4. Reconnect the ESXi hosts.
    a. Select **Hosts and Clusters** from the **Menu** drop-down menu.
    b. In the left pane, select **SA-Compute-01**.
    c. In the right pane, click the **Hosts** tab.

       If the ESXi hosts have a status of disconnected, perform substeps d through f.
    d. Right-click **sa-esxi-04.vclass.local** and select **Connection** > **Connect** if not connected.

       Perform substep d to reconnect sa-esxi-05.vclass.local and sa-esxi-06.vclass.local.
    e. Verify that all three ESXi hosts have a status of Connected.
    f. Reconnect any of the ESXi hosts (from Site A or Site B).

Task 4: Add ESXi Hosts to vCenter Server

You use the vSphere Client to add ESXi hosts to vCenter Server instance sa-vcsa-01.vclass.local.

1. In the vSphere Client, select **Menu > Hosts and Clusters**.
2. Add ESXi hosts to the vCenter Server inventory.
    a. Right-click **SA-Datacenter** and click **Add Host...**.
    b. On the Name and location page, enter **`sa-esxi-01.vclass.local`** and click **NEXT**.
    c. On the Connection settings page, enter user name **`root`** and password **`VMware1!`**, and click **NEXT**.

       If a security alert displays, accept the certificate by selecting **YES**.
    d. On the Host summary page, review the summary information and click **NEXT**.
    e. On the Assign license page, accept the default settings and click **NEXT**.
    f. On the Lockdown mode page, accept the default settings and click **NEXT**.
    g. On the VM location page, accept the default settings and click **NEXT**.
    h. On the Ready to complete page, review the information summary to add the host and click **FINISH**.

       After adding sa-esxi-01.vclass.local to the vCenter Server inventory, you must configure NTP on the host.

3. Configure NTP on the newly added ESXi host.
    a. In the vSphere Client, select **Menu > Hosts and Clusters**.
    b. In the navigation pane, select **sa-esxi-01.vclass.local** on the left side.
    c. Select **Configure > System > Time Configuration** in the right pane**.**
    d. Under Network Time Protocol settings, click **EDIT**.
    e. Select **Enable**.
    f. In the NTP Server box, enter **`172.20.10.10`**.
    g. Select **Start NTP Service**.
    h. For the NTP Service Startup Policy, use the drop-down menu and select **Start and stop with host**.
    i. Click **OK**.
4. Repeat steps 2 and 3 to add the ESXi host sa-esxi-02.vclass.local.
5. In the vSphere Client, select **Menu > Shortcuts**.

Lab 2 Configuring vSphere Distributed Switch

Objective and Tasks

Create and configure a distributed switch:

1. Create a Distributed Switch
2. Add ESXi Hosts to the Distributed Switch
3. Examine Your Distributed Switch Configuration
4. Migrate VMs to Another Distributed Switch Port Group

Task 1: Create a Distributed Switch

You create a distributed switch that functions as a single virtual switch across all associated hosts in your vSphere environment.

1. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar, and select **vSphere Client (SA-VCSA-01)**.

   If you are not logged in from a previous activity, log in using the vCenter Server lab credentials:

   User name **`administrator@vsphere.local`**
   Password **`VMware1!`**

2. Select **Menu > Networking**.
3. Right-click **SA-Datacenter** and select **Distributed Switch** > **New Distributed Switch**.

   The New Distributed Switch wizard appears.

4. Create a distributed switch.
    a. On the **Name and location** page, enter **dvs-Lab** in the **Name** blank and click **NEXT**.
    b. On the **Select version** page, leave **7.0.0 - ESXi 7.0 and later** selected and click **NEXT**.
    c. On the **Configure settings** page, enter **pg-SA-Production** in the Port group name blank, keep all other default values, and click **NEXT**.
    d. On the **Ready to complete** page, review the configuration settings and click **FINISH**.
5. In the left pane, expand **SA-Datacenter** and verify that the dvs-Lab distributed switch appears.
6. Configure the pg-SA-Production port group to use only Uplink 1.
    a. In the left pane, expand **dvs-Lab** distributed switch.
    b. Right-click **pg-SA-Production** port group and select **Edit Settings**.
    c. In the Edit Settings window, select **Teaming and failover**.
    d. Under the Failover Order section, move **Uplink 2**, **Uplink 3** and **Uplink 4** down until they appear under the Unused uplinks section.

    e. To apply these changes, click **OK**.

Task 2: Add ESXi Hosts to the Distributed Switch

You add ESXi hosts and physical adapters to the new distributed switch.

1. In the left pane, right-click **dvs-Lab** and select **Add and Manage Hosts...**.
2. On the **Select task** page, leave **Add hosts** selected and click **NEXT**.
3. On the **Select hosts** page, click **New hosts** (the green plus sign).
4. Select check boxes for the hosts listed here and click **OK**.

   sa-esxi-01.vclass.local
   sa-esxi-02.vclass.local
   sa-esxi-04.vclass.local
   sa-esxi-05.vclass.local
   sa-esxi-06.vclass.local

5. Click **NEXT**.
6. On the Manage physical adapters page, assign vmnic2 to Uplink 1 on sa-esxi-01, sa-esxi-02, sa-esxi-04, sa-esxi-05, and sa-esxi-06.
   a. Under sa-esxi-01.vclass.local, select **vmnic2** and click **Assign uplink**.
   b. Select **Uplink 1**.
   c. To apply this adapter assignment to all selected hosts, select **Apply this uplink assignment to the rest of the hosts** and click **OK**.

      Selecting this check box applies your physical adapter assignments to each host selected earlier through this wizard.

   d. When ready, click **NEXT**.
7. On the **Manage VMkernel adapters** page, click **NEXT**.
8. On the **Migrate VM networking** page, click **NEXT**.
9. On the **Ready to complete** page, review settings and click **FINISH**.

Task 3: Examine Your Distributed Switch Configuration

You examine distributed switch features, including the maximum transmission unit (MTU) value, VLAN capabilities, NetFlow, and Network I/O Control.

1. In the left pane, select **dvs-Lab**.
2. In the right pane, click the **Configure** tab and select **Settings > Topology**.
3. In the distributed switch topology diagram, expand **Uplink 1**.
4. Verify that the vmnic2 is attached and appears under Uplink 1 for ESXi hosts sa-esxi-01, sa-esxi-02, sa-esxi-04, sa-esxi-05, and sa-esxi-06.
5. Select **Settings > Properties** and verify the settings.
   - Network I/O Control is **Enabled**.
   - Number of uplinks is **4**.
   - The MTU size is **1500 Bytes**.
   - The Discover Protocol Type is set to **Cisco Discovery Protocol** and operation is set to **Listen**.
6. Click each remaining configuration link on the left under Settings to verify the current configuration.
   - LACP: No entries are in the main window.
   - Private VLAN: No entries are in the main window.
   - NetFlow: No Collector IP address is set in the main window.
   - Port Mirroring: No entries are in the main window.
   - Health Check: All items are set to **Disabled** in the main window.
7. In the left pane, select the **pg-SA-Production** port group.
8. In the right pane, click the **Configure** tab and select **Properties** on the left.
9. Verify the distributed port group settings in the main window.
   - General > Port binding, is set to Static binding.
   - General > Port allocation, is set to Elastic.
   - General > Number of ports, is set to 8.

Task 4: Migrate VMs to Another Distributed Switch Port Group

You move VMs from their current port groups on the dvs-SA-Datacenter distributed switch to the pg-SA-Production port group on the dvs-Lab distributed switch.

1. In the left pane, expand the **SA-Datacenter** and **dvs-SA-Datacenter** distributed switch.
2. Right-click **pg-SA-Management** and select **Migrate VMs to Another Network**.

   The Migrate VMs to Another Network wizard appears.
3. Migrate the VMs.
   a. In the Migrate VMs to Another Network page, for the Destination network click **BROWSE...**.
   b. Select **pg-SA-Production** and click **OK**.
   c. On the Select source and destination networks page, click **NEXT**.
   d. On the Select VMs to migrate page, select VMs **Linux01 & Linux02** and click **NEXT**.
   e. On the Ready to complete page, review settings and click **FINISH**.
   f. Monitor the task to completion using Recent Tasks.
4. Verify your distributed switch configuration.
   a. In the left pane, select **dvs-Lab** and click **Hosts** in the right pane.
   b. Verify that sa-esxi-01, sa-esxi-02, sa-esxi-04, sa-esxi-05, and sa-esxi-06 are connected to the distributed switch.

      The state of the ESXi hosts should be Connected.
   c. Click **VMs** and verify that the Linux01 and Linux02 VMs are listed.

      If the VMs are listed, they reside on the new distributed switch.
   d. Click **Ports** and verify that pg-SA-Production is listed in the Port Group column. Also verify that an uplink port group is listed which you previously mapped between vmnic2 and Uplink1.

      You can expand the Port Group column to view the full name of the uplink port group.
5. Select **Menu > Hosts and Clusters.**

6. Power on Linux01 and log in to its console.
   a. In the left pane, select **Linux01**.
   b. Right-click **Linux01** and select **Power** > **Power On**.
   c. In the right pane, click **Launch Web Console**.

      Wait for the VM to boot.
   d. Log in by entering user name **`root`** and password **`VMware1!`**.
7. At the command prompt, ping 172.20.10.10 (the domain controller's IP address) to verify that the VM has full network connectivity.

   ```
   ping -c 3 172.20.10.10
   ```
8. If the `ping` command is successful, continue to Step 10.
9. If the `ping` command is unsuccessful, restart the networking in the VM.
   a. Enter the command to ensure that your VM has a valid DHCP-assigned IP address.

      ```
      service network restart
      ```
   b. Repeat steps 7 and 8.
10. Close the VM **Linux01** web console tab.
11. In the vSphere Client, select **Menu > VMs and Templates**.

Lab 3 Managing vSphere Distributed Switches

Objective and Tasks

Perform a health check, remediate the vSphere Distributed Switch (VDS) issue and back up a distributed switch:

1. Add a New Port Group to VDS
2. Enable the VDS Health Check
3. Investigate the VDS Health Check Status
4. Remediate the VDS Issue
5. Disable the VDS Health Check Service
6. Back Up the VDS Configuration

Task 1: Add a New Port Group to VDS

You add a port group to the dvs-Lab vSphere distributed switch.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. Select **Menu > Networking**.
3. In the left pane, select the VDS **dvs-Lab**.
4. Right-click **dvs-Lab** and select **Distributed Port Group > New Distributed Port Group**.

5. On the Name and location page, enter **pg-SA-Testing** in the **Name** text box and click **NEXT**.
6. On the Configure settings page, select **VLAN** under VLAN type from the drop-down menu, enter **10** for the VLAN number, and click **NEXT**.
7. On the Ready to complete page, review the information about your new DVS port group and click **FINISH**.

Task 2: Enable the VDS Health Check

You enable the VDS health check service on the dvs-Lab vSphere distributed switch to verify its configuration for errors or mismatches.

1. Select **Menu > Networking**.
2. In the left pane, select **dvs-Lab**.
3. In the right pane, click **Configure** > **Health Check** on the left.
4. Click **Edit** in the top-right corner.
5. Under VLAN and MTU, select **Enabled** from the **State** drop-down menu.
6. Under Teaming and failover, select **Enabled** from the **State** drop-down menu.
7. Click **OK**.

NOTE

After the health check is enabled, the VDS health check begins testing for selected configuration options (VLAN and MTU, Teaming and Failover, or both) by creating many fictitious MAC addresses. These MAC addresses continue to be created and sent through the vSphere and physical networks as long as the VDS health check is enabled.

Task 3: Investigate the VDS Health Check Status

You check for results from the VDS health check service.

The health check can take some time.

1. Select **dvs-Lab** in the left pane.
2. Select **Monitor > Health** in the right pane.
3. Observe the Host Name list in the right pane.

   This list should comprise all hosts that were added to vSphere Distributed Switch.

   This list continuously updates with health check results while the health check service is enabled.
4. Highlight a host listing, where a warning appears, to view the additional information displayed below it.

   VLAN is the default tab under Health status details. To check MTU or other settings, you must click the individual tabs.

   When you set a VLAN in task 1, it was a bad VLAN because it is a mismatch to the physical environment.

Task 4: Remediate the VDS Issue

You fix the bad VLAN configured on your new port group that you confirmed through the VDS health check.

1. Expand the **dvs-Lab** vSphere distributed switch.
2. Right-click the **pg-SA-Testing** port group and select **Edit settings...**.
3. On the VLAN page, select **None** for the setting VLAN type.

   Selecting **None** for this value removes any previously applied VLAN tags on the pg-SA-Testing port group.

   NOTE

   VMkernel port configuration is managed independently. However, VDS port group configuration can affect VMkernel port configuration.

   ---

4. To apply the VLAN change, click **OK**.
5. Verify your change.
   a. Select **Monitor > Health** and verify that VLAN Health Status has changed and now indicates Normal.

Task 5: Disable the VDS Health Check Service

You disable the VDS health check service on the dvs-Lab vSphere distributed switch.

Disabling the VDS health check service is important because of the many fictitious MAC addresses generated at one-minute intervals to facilitate troubleshooting efforts in the network infrastructure. The environment will need time for those MAC addresses to time out of the infrastructure, according to the network policy after the VDS health check is disabled.

1. Select **Menu > Networking**.
2. In the left pane, select VDS **dvs-Lab**.
3. In the right pane, click **Configure** > **Health Check** on the left.
4. Click **Edit**.
5. Under VLAN and MTU, select **Disabled** from the **State** drop-down menu.
6. Under Teaming and failover, select **Disabled** from the **State** drop-down menu.
7. Click **OK**.

Task 6: Back Up the VDS Configuration

You back up the configuration for the dvs-Lab vSphere distributed switch.

1. In the left pane, right-click **dvs-Lab** and select **Settings** > **Export Configuration**.
2. In the Export Configuration dialog box, leave **Distributed switch and all port groups** selected and click **OK**.
3. Save the distributed switch configuration to the desktop with the filename `dvs-Lab-backup.zip`.
4. In the vSphere Client, select **Menu > Global Inventory Lists.**

Lab 4 Using Port Mirroring

Objective and Tasks

Configure port mirroring and capture network traffic on a distributed switch:

1. Prepare to Capture Mirrored Network Traffic
2. Configure Port Mirroring on the Distributed Switch
3. Verify That Port Mirroring Is Capturing Traffic
4. Restore the Distributed Switch Configuration

Task 1: Prepare to Capture Mirrored Network Traffic

You use the Linux01 VM to capture and monitor mirrored traffic.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. Select **Menu > Hosts and Clusters**.
3. In the left pane, expand **SA-Datacenter** and expand **SA-Compute-01**.
4. In the left pane, select the **Linux01** VM.

   The Linux01 VM is used for traffic capture.
5. In the right pane, click **Summary** and click **Launch Web Console**.

6. In the Linux01 web console, enter the `tcpdump` command at the command prompt.

   `tcpdump -nn icmp`

   This command line is used to monitor ICMP network traffic.

7. Monitor the command output for a few seconds and verify that ICMP traffic is not being captured.

   The `tcpdump` output does not have any information to display until ICMP traffic is detected on the network.

8. Leave the console window open with the `tcpdump` command running uninterrupted.
9. Return to the **vSphere Client** tab.
10. Power on the Linux02 VM and log in to its console.
    a. In the left pane, select **Linux02**.
    b. Right-click **Linux02** and select **Power** > **Power On**.
    c. In the right pane, click **Summary** and click **Launch Web Console**.
    d. Click the Linux02 **Web Console** tab in the browser and click in the window to capture keyboard input.

       Wait for the VM to fully boot.

    e. Log in by entering user **`root`** with password **`VMware1!`** .

       The Linux02 VM is used as the traffic source to be monitored.

11. At the Linux02 command prompt, enter the `ping` command.

    `ping 172.20.10.10`

    This command pings the default router IP address.

12. If the `ping` command does not work, enter the following command to restart network services and then repeat step 11.

    `service network restart`

13. After the `ping` command begins to work, click the **Linux01** console tab.
14. In the Linux01 console window, verify that the running `tcpdump` command output remains silent and did not capture any ICMP traffic.

Task 2: Configure Port Mirroring on the Distributed Switch

You configure port mirroring so that the port connected to the Linux02 VM is the mirror source and the port connected to the Linux01 VM is the mirror destination.

All the traffic present on the Linux02 port is forwarded to the Linux01 port for examination.

1. From the vSphere Client, select **Menu > Networking.**
2. In the left pane, expand **SA-Datacenter** and select **dvs-Lab**.
3. In the right pane, click **Configure** and select **Port Mirroring** on the left.
4. Add a port mirroring session.
   a. In the Port Mirroring panel, click **+New**.

      The Add Port Mirroring Session wizard appears.

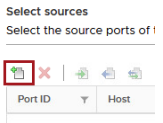
   b. On the Select session type page, accept the default **Distributed Port Mirroring** and click **NEXT**.

      When you select this session type, distributed ports can only be local. If the source and destination ports are on different hosts, port mirroring does not work between them.

      Ensure that the Linux01 and Linux02 VMs both reside on sa-esxi-04.vclass.local.

   c. On the Edit properties page, configure the port mirroring session.
      i. From the **Status** drop-down menu, select **Enabled**.
      ii. From the **Normal I/O on destination ports** drop-down menu, select **Allowed** and click **NEXT.**

   d. On the Select sources page, configure the port mirroring source.
      i. Click the **Select distributed ports to add to this port mirroring session** icon.



      ii. In the Select Ports dialog box, select **Linux02** and click **OK**.
      iii. Click **NEXT**.

   e. On the Select destinations page, configure the port mirroring destination.
      i. Click the **Select distributed ports to add to this port mirroring session** icon.
      ii. In the Select Ports dialog box, select **Linux01** and click **OK**.
      iii. Click **NEXT**.

f. On the Ready to complete page, review settings and click **FINISH**.

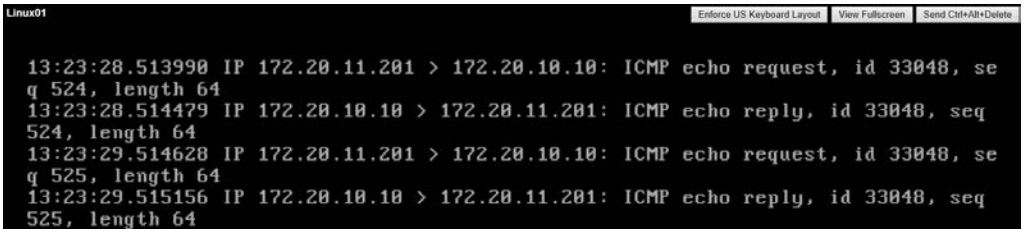
g. Monitor to completion using Recent Tasks.

Task 3: Verify That Port Mirroring Is Capturing Traffic

With port mirroring configured, you view the `tcpdump` command output and verify that any ICMP traffic appearing on the Linux02 port is duplicated on the Linux01 port.

1. Return to the **Linux02** console tab.
2. Verify that the `ping` command is still reaching the default router IP address.
3. Go to the **Linux01** console tab.
4. In the Linux01 console, examine the `tcpdump` output in the terminal window.

   The output looks similar to the following screenshot.



5. Record the local address that appears in the captured traffic.

   _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

   The local address begins with 172.20.11.

6. In the Linux01 console window, press Ctrl+C to stop the `tcpdump` command.

   a. If pressing Ctrl+C does not work, click anywhere inside the tab screen and repeat.

7. Click the **Linux02** console tab.
8. In the Linux02 console window, press Ctrl+C to stop the `ping` command.
9. At the Linux02 command prompt, use `ifconfig` to examine the IP configuration.

   `ifconfig`

10. Use the command output to verify that the Linux02 IP address matches the address that you recorded in step 5.
11. Close the **Linux01** and **Linux02** console tabs.
12. Shut down Linux01 and Linux02.
    a. In your vSphere Client, select **Hosts and Clusters** from the **Menu** drop-down menu.
    b. In the left pane, right-click **Linux01** and select **Power** > **Shut Down Guest OS**.
    c. In the pop-up window, click **Yes** to confirm the shutdown operation.
    d. Repeat substeps b and c to shut down **Linux02**.

Task 4: Restore the Distributed Switch Configuration

You restore the VDS dvs-Lab configuration to reset any configuration change made since the configuration was saved.

1. Select **Menu > Networking**.
2. In the left pane, right-click VDS **dvs-Lab** and select **Settings** > **Restore Configuration**.

   The Restore Configuration wizard appears.
3. On the Restore switch configuration page, click **BROWSE**, select the file `dvs-Lab-backup.zip`, and click **Open**.
4. Leave **Restore distributed switch and all port groups** selected and click **NEXT**.
5. On the Ready to complete page, review the settings and click **FINISH**.
   a. If you lose connection to the vSphere Client, restart Firefox.
6. After the switch configuration is restored, verify the configuration.
   a. If the switch configuration did not restore properly, repeat steps 1 through 5.
   b. View the port mirroring configuration and verify that the VDS dvs-Lab has no sessions configured.

      The port mirroring configuration was removed by the VDS restore operation.
7. In the vSphere Client, select **Menu > Home**.

Lab 5 Using Policy-Based Storage

Objective and Tasks

Use policy-based storage to create tiered storage:

1. Add Datastores for Use by Policy-Based Storage
2. Use vSphere Storage vMotion to Migrate a VM's Storage
3. Configure Storage Tags
4. Create VM Storage Policies
5. Assign Storage Policies to VMs

Task 1: Add Datastores for Use by Policy-Based Storage

You create two small datastores, as simple tiered storage, for use by your vCenter Server instance.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. Select **Menu > Storage**.

3. Create a datastore named ds-gold.
    a. In the left pane, right-click **SA-Datacenter** and select **Storage** > **New Datastore**.

       The New Datastore wizard appears.
    b. On the Type page, leave **VMFS** selected and click **NEXT**.
    c. On the Name and device selection page, enter **`ds-gold`** in the **Datastore name** text box.
    d. From the **Select a host...** drop-down menu, select ESXi host **sa-esxi-04.vclass.local**.
    e. From the LUN list, select the entry description **FreeNAS ISCSI Disk (naa..)** with capacity **8.00 GB**, and click **NEXT**.

       Local drives are labeled as Local VMware Disk. Do not select these drives.

       If iSCSI devices are not present, ask the instructor for instructions to add them.
    f. On the VMFS version page, leave **VMFS 6** selected and click **NEXT.**
    g. On the Partition configuration page, keep the default values and click **NEXT.**
    h. On the Ready to complete page, review settings and click **FINISH**.
    i. In the left pane, expand **SA-Datacenter** and verify that the datastore ds-gold appears.
4. Create a datastore named ds-silver.
    a. In the left pane, right-click **SA-Datacenter** and select **Storage** > **New Datastore**.

       The New Datastore wizard appears.
    b. On the Type page, leave **VMFS** selected and click **NEXT**.
    c. On the Name and device selection page, enter **`ds-silver`** in the **Datastore name** text box.
    d. From the **Select a host...** drop-down menu, select ESXi host **sa-esxi-04.vclass.local**.
    e. From the LUN list, select the entry description **FreeNAS ISCSI Disk (naa..)** with capacity **12.00 GB**, and click **NEXT**.

       Local drives are labeled as Local VMware Disk. Do not select these drives.
    f. On the VMFS version page, leave **VMFS 6** selected and click **NEXT**.
    g. On the Partition configuration page, keep the default values and click **NEXT**.
    h. On the Ready to complete page, review settings and click **FINISH**.
    i. Verify that the datastore ds-silver appears in the left pane.

Task 2: Use vSphere Storage vMotion to Migrate a VM's Storage

You use vSphere Storage vMotion to migrate the Photon-01 VM to the ds-gold datastore.

1. Select **Menu > Hosts and Clusters**.
2. In the left pane, right-click **Photon-01** and select **Migrate**.

   The Migrate wizard appears.
3. On the Select a migration type page, click **Change storage only** and click **NEXT**.
4. On the Select storage page, select the datastore **ds-gold**, leave all other settings with their default values, and click **NEXT**.
5. On the Ready to complete page, click **FINISH**.
6. In the Recent Tasks pane, monitor the migration task to completion.
7. Verify that the migration was successful.

   You might need to refresh the vSphere Client to see that the migration is complete.

   a. In the left pane, select **Photon-01**.

   b. In the right pane, click the **Datastores** tab and verify that the ds-gold datastore is listed.

Task 3: Configure Storage Tags

You create the tags necessary to implement simple tiering.

The Storage Tiers tag category contains the Gold and Silver identifier tags associated with individual datastores.

1. Select **Menu > Tags & Custom Attributes**.
2. In the right pane, click the **Tags** tab.
3. Configure a new tag category and the Gold Tier identifier tag.

   a. In the Tags panel, click **NEW**.

   b. In the **Name** text box, enter **`Gold Tier`**.

   c. Click the **Create New Category** link next to the **Category** drop-down menu.

      A dialog box appears that includes tag and category configuration options.

      Categories can be created only as part of the identifier tag creation process.

   d. In the **Category Name** text box, enter **`Storage Tiers`**.

   e. Keep the default values for the remaining settings and click **CREATE**.

   f. In the Create Tag dialog box, click **CREATE**.

4. Create a Silver Tier identifier tag.
   a. In the Tags panel, click **NEW**.
   b. In the **Name** text box, enter **`Silver Tier`**.
   c. Select **Storage Tiers** from the **Category** drop-down menu and click **CREATE**.
5. Assign the Gold Tier tag to the ds-gold datastore.
   a. Select **Menu > Storage**.
   b. In the left pane, right-click **ds-gold** and select **Tags & Custom Attributes** > **Assign Tag**.
   c. Select the **Gold Tier** tag and click **ASSIGN**.
   d. In the left pane, select **ds-gold**.
   e. In the Tags panel on the **Summary** tab, verify that the Gold Tier tag is associated with the ds-gold datastore.
6. Assign the Silver Tier tag to the ds-silver datastore.
   a. In the left pane, right-click the **ds-silver** datastore and select **Tags & Custom Attributes** > **Assign Tag**.
   b. Select the **Silver Tier** tag and click **ASSIGN**.
   c. In the left pane, select the datastore **ds-silver**.
   d. In the Tags panel on the **Summary** tab, verify that the Silver Tier tag is associated with the ds-silver datastore.

Task 4: Create VM Storage Policies

You assign storage policies to VMs and you specify the configuration settings to be enforced.

1. Select **Menu > Policies and Profiles.**
2. In the left pane, click **VM Storage Policies**.
3. Create a Gold Tier storage policy.
   a. In the VM Storage Policies panel, click **Create VM Storage Policy**.

      The Create VM Storage Policy wizard appears.
   b. On the Name and description page, enter **`Gold Tier Policy`** in the **Name** text box and click **NEXT**.
   c. On the Policy structure page, select **Enable tag based placement rules** and click **NEXT**.

d. On the Tag based placement page, select **Storage Tiers** from the Tag category drop-down menu.

e. Click **BROWSE TAGS**, select **Gold Tier**, click **OK**, and click **NEXT**.

f. On the Storage compatibility page, verify that the datastore ds-gold is listed under Compatible storage and click **NEXT**.

g. On the Review and finish page, click **FINISH**.

4. Repeat step 3 to create Silver Tier Policy by using the Silver Tier tag.
5. Verify that Gold Tier Policy and Silver Tier Policy are entries in the Name column.
   a. If the entries cannot be found, repeat any steps needed to add the entries.

Task 5: Assign Storage Policies to VMs

You assign the Gold and Silver storage policies to individual VMs and you mitigate compliance issues.

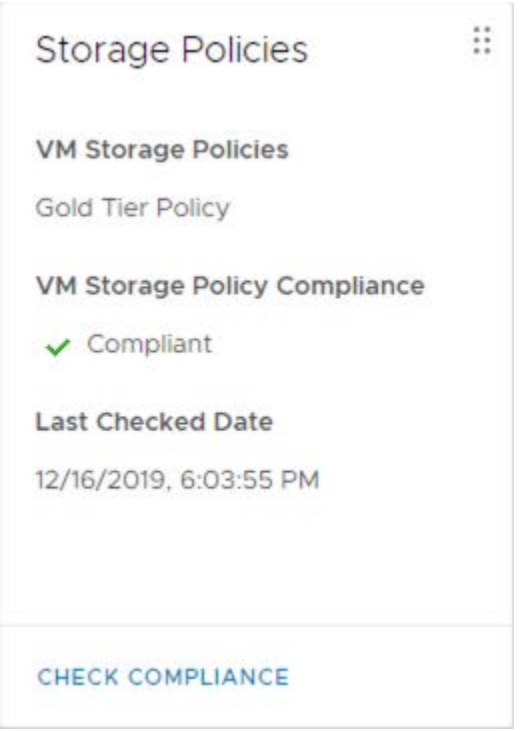
A storage policy can be assigned to a VM while the VM is powered on or powered off.

1. Select **Menu > Hosts and Clusters**.
2. In the left pane, expand **SA-Datacenter** and the cluster **SA-Compute-01**.
3. Apply the Gold Tier storage policy to the Photon-01 VM.
   a. Right-click **Photon-01** and select **VM Policies** > **Edit VM Storage Policies**.
   b. On the Edit VM Storage Policies page, select **Gold Tier Policy** from the **VM storage policy** drop-down menu and click **OK**.
   c. In the left pane, select **Photon-01**.
   d. In the right pane, click the **Summary** tab.

e. Scroll down and expand the **Storage Policies** panel, if necessary.

f. Verify that Gold Tier Policy appears and that Photon-01 is compliant.

The Photon-01 VM is compliant because it was already moved to a policy-appropriate datastore.



4. Apply the Silver Tier storage policy to the Photon-02 VM.

a. In the left pane, right-click **Photon-02** and select **VM Policies** > **Edit VM Storage Policies**.

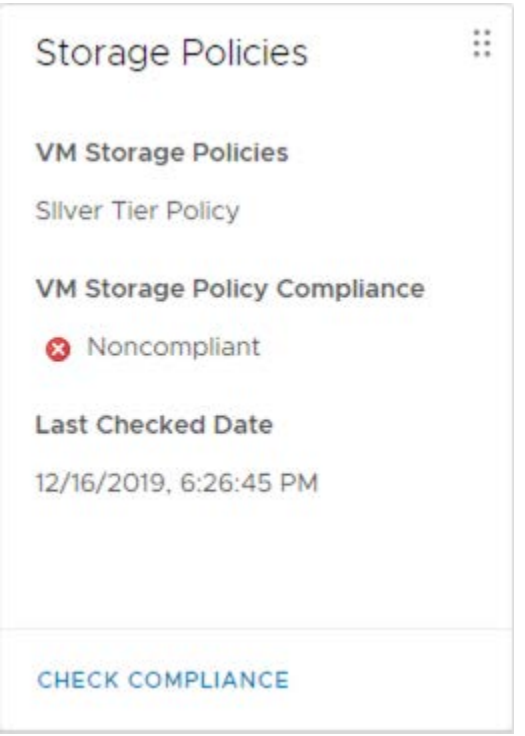
b. On the Edit VM Storage Policies page, select **Silver Tier Policy** from the **VM storage policy** drop-down menu and click **OK**.

c. In the left pane, select **Photon-02**.

d. In the right pane, click the **Summary** tab.

e. View the VM Storage Policies panel, verify that Silver Tier Policy appears and that Photon-02 is noncompliant.

The Photon-02 VM is noncompliant because its virtual disk is stored on a datastore that is not tagged as a part of the assigned policy.



5. Remediate the compliance issue for Photon-02.

a. In the left pane, right-click **Photon-02** and select **Migrate**.

The Migrate wizard appears.

b. On the Select a migration type page, click **Change storage only** and click **NEXT**.

c. On the Select storage page, select datastore **ds-silver** and click **NEXT**.

With a VM storage policy assigned to the Photon-02 VM, datastores are listed as either Compatible or Incompatible.

d. On the Ready to complete page, review the migration details and click **FINISH**.

e. In the Recent Tasks pane, monitor the migration task to completion.

The migration must complete successfully.

6. Verify that Photon-02 is reported as compliant.
   a. In the right pane, verify that the status in the VM Storage Policies panel is Compliant.
   b. If the status is not Compliant, click the **Check Compliance** link in the VM Storage Policies panel.
   c. Verify that the status changes to Compliant.
7. In the vSphere Client, select **Menu > Shortcuts**.

Lab 6 Creating vSAN Storage Policies

Objective and Tasks

Create and review vSAN storage policies:

1. Examine the Default Storage Policy
2. Create a Custom Policy with No Failure Tolerance
3. Assign the Custom Policy to a VM
4. Make the VM Compliant
5. Create an Invalid Storage Policy

Task 1: Examine the Default Storage Policy

You examine the vSAN default storage policy.

A vSAN datastore has been preconfigured for you.

1. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar, and select **vSphere Client (SA-VCSA-01)**.
    a. If you are not logged in from a previous activity, log in using the vCenter Server lab credentials.
2. Select **Menu > Policies and Profiles.**
3. In the left pane, select **VM Storage Policies**.

4. In the right pane, select **vSAN Default Storage Policy** and click **Edit Settings**.
5. On the Name and description page, click **NEXT**.
6. On the vSAN page, examine the rules under the **Availability**, **Advanced Policy Rules**, and **Tags** tabs.

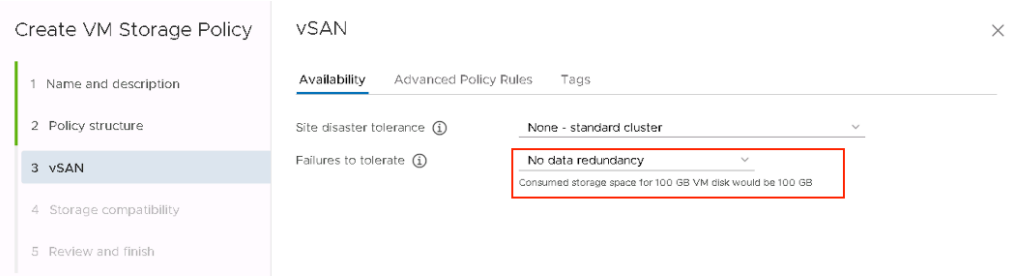
   Q1. How many failures can be tolerated?
7. Click **CANCEL**.

Task 2: Create a Custom Policy with No Failure Tolerance

You create a custom vSAN storage policy that does not provide failure tolerance.

1. In the right pane, click **Create VM Storage Policy**.
2. On the Name and description page, enter **`vSAN-VM-Custom-Policy-FTT0`** in the **Name** text box and click **NEXT**.
3. On the Policy structure page, select the **Enable rules for "vSAN" storage** check box and click **NEXT**.
4. On the vSAN page **Availability** tab under Failures to tolerate, select **No data redundancy** from the drop-down menu.

   View the consumed storage space information below the drop-down menu.



   Q1. Why is the storage space size equal to the VM size?
5. To complete the vSAN page, click **NEXT**.
6. On the Storage compatibility page, click **NEXT**.

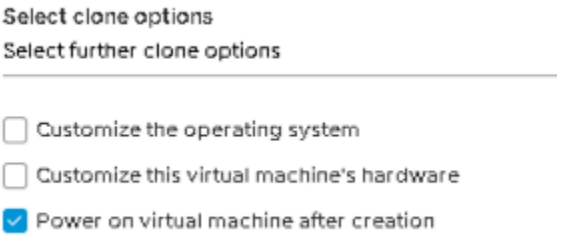
   Only the vSAN datastore is listed under Compatible storage.
7. On the Review and finish page, click **FINISH**.
8. Verify that the vSAN-VM-Custom-Policy-FTT0 storage policy is created and appears in the list.

   You might need to scroll through the VM Storage Policies list.

Task 3: Assign the Custom Policy to a VM

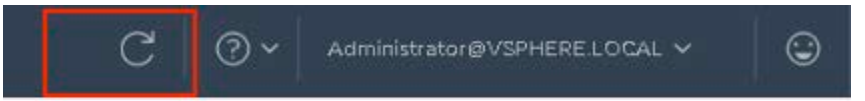
You create a second VM and apply your new vSAN storage policy.

1. In the vSphere Client, Select **Menu > Hosts and Clusters**.
2. Clone a VM from Photon-01.
   a. In the left pane, right-click **Photon-01** and select **Clone** > **Clone to Virtual Machine**.
   b. On the Select a name and folder page, enter **`Payload-02`** in the **Virtual machine name** text box and click **NEXT**.
   c. On the Select a compute resource page, expand **SA-Compute-01**, select **sa-esxi-05.vclass.local**, and click **NEXT**.
   d. On the Select storage page, select **Datastore Default** from the **VM Storage Policy** drop-down menu.
   e. Select **OPSCALE-Datastore** from the datastore list and click **NEXT**.
   f. On the Select clone options page, select only **Power on virtual machine after creation** and click **NEXT**.



   g. On the Ready to complete page, click **FINISH**.
   h. Monitor the Recent Tasks pane to verify that the Clone virtual machine task completes successfully.
3. Verify that your new VM is listed in the left pane and is powered on.

   If you do not see the VM listed and powered on, click the **Refresh** icon.



4. Assign the vSAN-VM-Custom-Policy-FTT0 storage policy to Payload-02.
    a. In the left pane, right-click **Payload-02** and select **VM Policies** > **Edit VM Storage Policies**.
    b. Select **vSAN-VM-Custom-Policy-FTT0** from the **VM storage policy** drop-down menu.
        Q1. Why do the VM home and Hard disk 1 objects have warning icons?
    c. Click **OK**.
    d. Monitor the Recent Tasks pane to verify that the Reconfigure virtual machine task completes successfully.
5. In the left pane, select **Payload-02**.
6. On the **Summary** tab, review the Related Objects panel and the VM Storage Policies panel.

    You might need to scroll down in the right pane to see these panels.

    Q2. On which datastore is the VM located?

    Q3. Which storage policy is the VM using?

    Q4. Is the VM compliant with its storage policy?

Task 4: Make the VM Compliant

You migrate the Payload-02 VM from the shared VMFS datastore to the vSAN datastore to make it compliant with its storage policy.

1. Migrate the Payload-02 VM to the vSAN datastore to ensure its compliance.
    a. In the left pane, right-click **Payload-02** and select **Migrate**.
    b. On the Select a migration type page, click **Change storage only** and click **NEXT**.
    c. On the Select Storage page, leave **Keep existing VM storage policies** selected in the **VM Storage Policy** drop-down menu.
    d. In the datastore list, select **vsanDatastore** and click **NEXT**.
    e. On the Ready to complete page, click **FINISH**.
    f. Monitor the Recent Tasks pane until the task completes successfully.

2. In the right pane, view the VM Storage Policies panel and click **Check Compliance**.

   The compliance status might have been refreshed automatically by the vSphere Client. If so, clicking **Check Compliance** is not required.

3. Verify that the compliance status of Payload-02 changes to Compliant.

Task 5: Create an Invalid Storage Policy

You create a storage policy that is invalid for the vSAN datastore and you apply it to a VM.

The purpose of this task is to provide another example of the warning messages that appear when an invalid storage policy is created.

1. Select **Menu > Policies and Profiles**.
2. In the left pane, click **VM Storage Policies**.
3. Create a vSAN storage policy.
   a. In the right pane, click **Create VM Storage Policy**.
   b. On the Name and description page, enter **RAID5** in the **Name** text box and click **NEXT**.
   c. On the Policy structure page, select the **Enable rules for "vSAN" storage** check box and click **NEXT**.
   d. On the vSAN page under the **Availability** tab, select **1 failure - RAID-5 (Erasure Coding)** from the **Failures to tolerate** drop-down menu and click **NEXT**.
   e. On the Storage compatibility page, click **NEXT**.

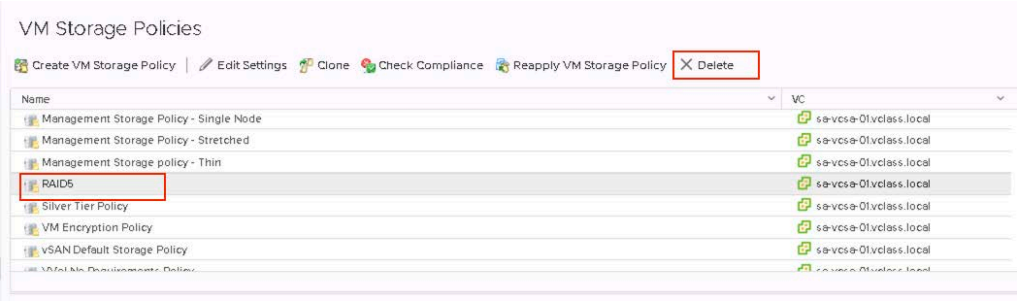
      Compatible datastores do not exist.

   f. On the Review and finish page, click **FINISH**.
4. Assign the RAID5 storage policy to Payload-02.
   a. Select **Menu > Hosts and Clusters**.
   b. In the left pane, right-click **Payload-02** and select **VM Policies** > **Edit VM Storage Policies**.
   c. Select **RAID5** from the **VM storage policy** drop-down menu.

      Q1. Why do the VM home and Hard disk 1 objects have warning icons?

5. Click **CANCEL**.

6. Select **Menu > Policies and Profiles**.
7. In the left pane, click **VM Storage Policies**.
8. In the right pane, select **RAID5** and click **Delete**.



9. On the Delete VM Storage Policy page, click **OK**.
10. In the vSphere Client, select **Menu > Home**.

Lab 7 Working with Certificates

Objective and Tasks

Generate and replace a vCenter Server certificate using the vSphere Client:

1. Examine the Machine SSL Certificate
2. Generate a CSR for the Custom Certificate
3. Request a Custom Certificate
4. Replace the Current Certificate with a Custom Certificate

Task 1: Examine the Machine SSL Certificate

You investigate the vCenter Server machine SSL certificate using the vSphere Client.

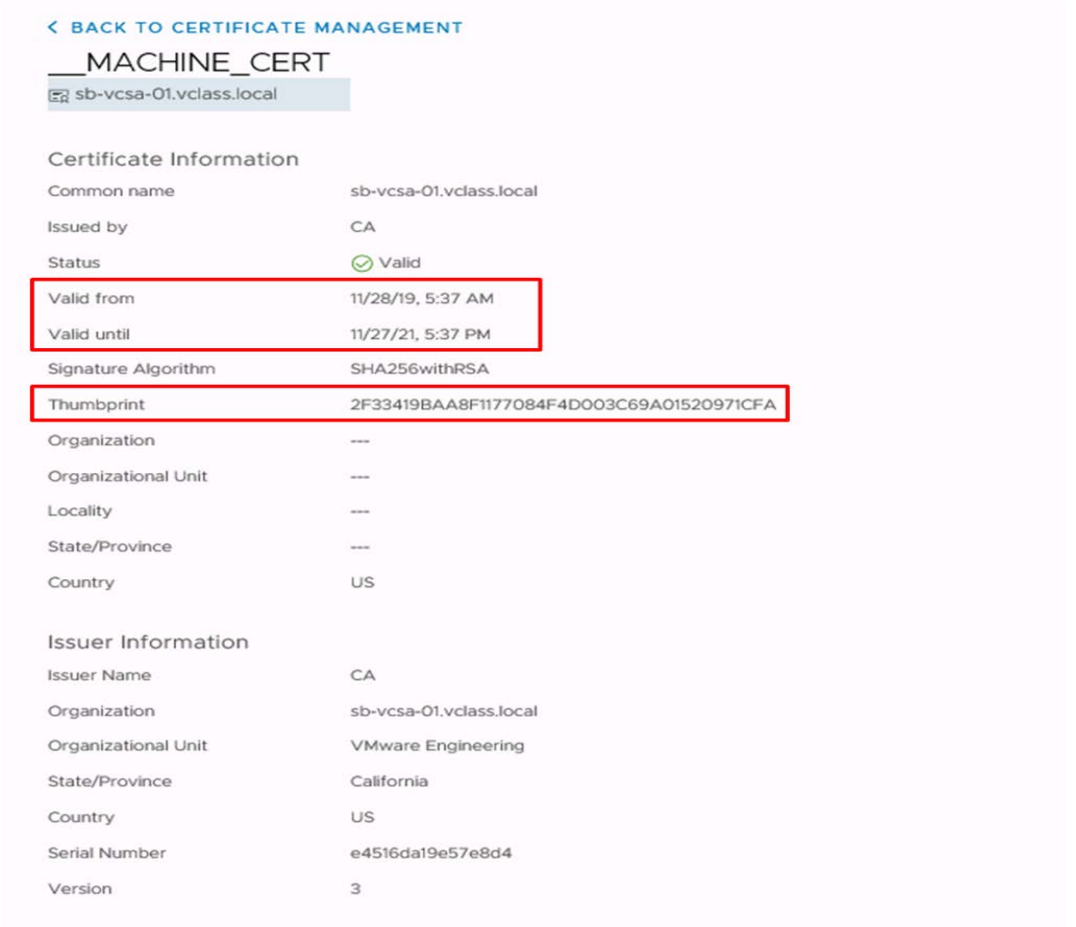
1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. Select **Menu > Administration**.
3. Select **Certificates > Certificate Management**.
4. On the **Certificate Management** page, select **SA-VCSA-01.VCLASS.LOCAL** from the **vCenter Server** drop-down menu in the top-right corner.

5. Click **VIEW DETAILS** to see details for the machine SSL certificate.

NOTE

The following screenshot is an example. Your certificate information will be different.



6. Record the following certificate information for future comparison.

   Valid from: _____
   Valid until: _____

   Thumbprint: _____

   Each time a certificate is renewed, the current time is set as the **Valid from** time and the **Valid to** time is set as 2 years from that moment.
   The certificate thumbprint, also called a cert hash, is unique and changes with each certificate generated.

7. When you have finished reviewing the Machine SSL certificate details, click **< BACK TO CERTIFICATE MANAGEMENT** at the top of the page.

8. Scroll down and click **VIEW DETAILS** for the first certificate under Trusted Root Certificates.

   Q1. Who issued the certificate?

9. When you have finished reviewing the Trusted Root certificate details, click **< BACK TO CERTIFICATE MANAGEMENT** to return to Certificate Management.

Task 2: Generate a CSR for the Custom Certificate

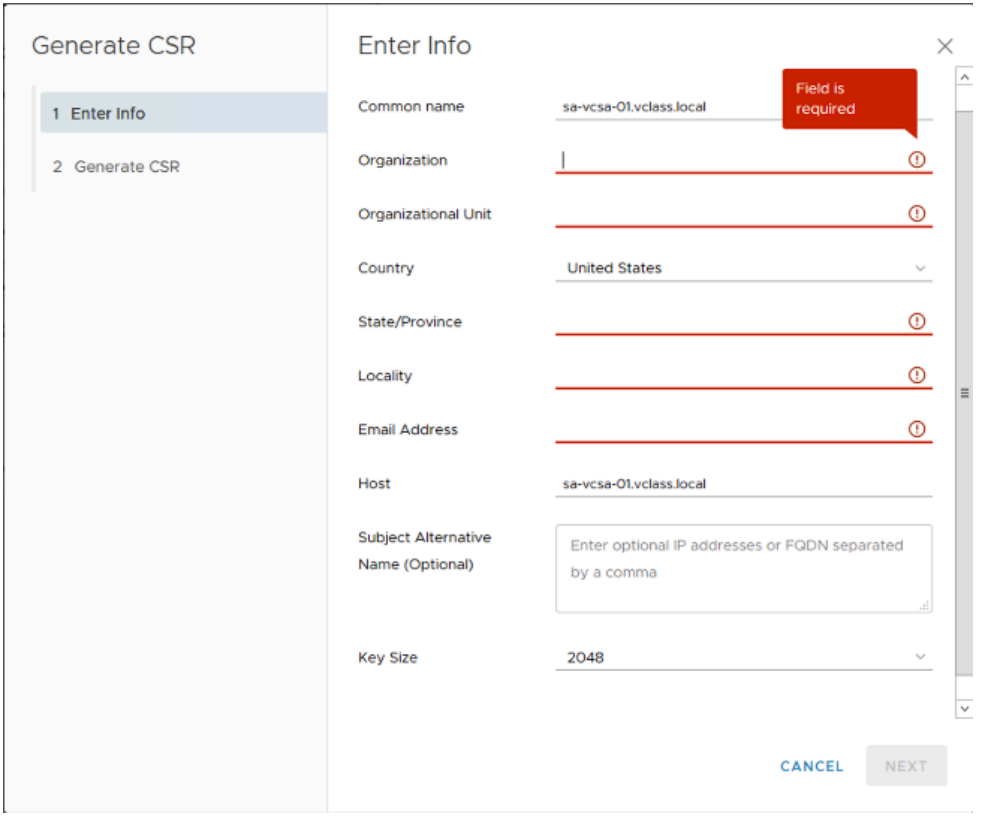
You use the vSphere Client to generate a certificate signing request (CSR) for the custom certificate.

1. Generate the CSR.

   a. Under Machine SSL Certificate, click **Actions** > **Generate Certificate Signing Request (CSR)**.

   b. Enter the required details to finish the certificate signing request.

      Organization : **VMware**
      Organizational Unit: **Education**
      State/Province: **California**
      Locality: **Palo Alto**
      Email Address: **cert.admin@vmware.com**



c. When finished, click **NEXT**.

2. Click **DOWNLOAD** on the Generate CSR screen to capture the CSR into a `sa-vcsa-01.vclass.local.csr` file and save the file to the `C:\Materials\Downloads` folder.

3. Click **FINISH** to close the wizard.

   After creating the certificate signing request, you must provide it to your Certificate Authority to receive a CA-signed custom certificate. You will do this in the next task.

Task 3: Request a Custom Certificate

You request a custom certificate from the vclass.local domain.

1. Prepare the certificate signing request info.
    a. On your student desktop, open **Windows Explorer** and navigate to the `C:\Materials\Downloads` folder.
    b. Right-click the `sa-vcsa-01.vclass.local.csr` file and select **Edit with Notepad++**.

       If a pop-up window appears indicating that there is an update regarding the Notepad++ application, do not update. Instead, continue the task.
    c. Select all text from the contents of the `sa-vcsa-01.vclass.local.csr` file.

       Do not include any additional spaces.
    d. Copy the selected text to the clipboard.
    e. Minimize the Notepad++ window.
    f. Minimize the Windows Explorer window.
2. Request a certificate from the Certificate Authority.
    a. On your student desktop, open a new Firefox tab and select **Infrastructure > Certificate Services (vClass.local)** from the bookmark bar or go to **`http://dc.vclass.local/certsrv`**.
    b. Log in by entering user name **`administrator`** and password **`VMware1!`** .
    c. On the Microsoft Active Directory Certificate Services page, click **Request a certificate**.
    d. Click the **advanced certificate request** link.
    e. Under Saved Request, paste the CSR text from step 1 into the **Base-64-encoded certificate request** text box.
    f. From the **Certificate Template** drop-down menu, select **vSphere 7**.
    g. Click **Submit**.
    h. Click **Base 64 encoded**.
    i. Click **Download certificate**.
    j. Save the file to the folder `C:\Materials\Downloads` as **`machine_ssl.cer`**.

3. Download the certificate chain.
    a. On the **Firefox** tab, click **Download certificate chain**.

       Base 64 encoded should still be selected.

    b. Save the output file to the `C:\Materials\Downloads` as the file **`cachain.p7b`** folder.

    c. Close the **Microsoft Active Directory Certificate Services** tab.

    d. Close **Notepad++**.

4. Export the root certificate.
    a. Switch to Windows Explorer and navigate to the `C:\Materials\Downloads` directory.

    b. Right-click the file **cachain.p7b** and select **Open**.

       The Certificate Manager Console opens.

    c. In the left pane, expand the inventory tree until you see the folder `Certificates`.

    d. Select **Certificates**.

       You should see two certificates in the right pane: the root certificate for your domain controller (vclass-DC-CA) and the custom certificate for your vCenter Server Appliance instance (sa-vcsa-01.vclass.local).

       For the custom CA-signed certificate issued to sa-vcsaa-01.vclass.local, vSphere 7 appears under the Certificate Template column on the far right side.

    e. To export the root certificate, right-click the root certificate **vclass-DC-CA**, and select **All Tasks** > **Export**.

       The Certificate Export Wizard appears.

    f. Click **Next**.

    g. On the Export File Format page, select **Base-64 encoded X.509 (.CER)** and click **Next**.

    h. On the File to Export page, click **Browse**.

    i. Navigate to the folder `C:\Materials\Downloads`.

    j. In the **File name** text box, enter **`root-64`**.

    k. Click **Save**.

l. On the File to Export page, click **Next**.

m. On the Completing the Certificate Export Wizard page, click **Finish**.

n. On the Certificate Export Wizard window, click **OK**.

o. Close the Certificate Manager Console.

p. Close the Windows Explorer.

Task 4: Replace the Current Certificate with a Custom Certificate

You import and replace the VMware CA self-signed certificate with an external CA-signed certificate using the vSphere Client.

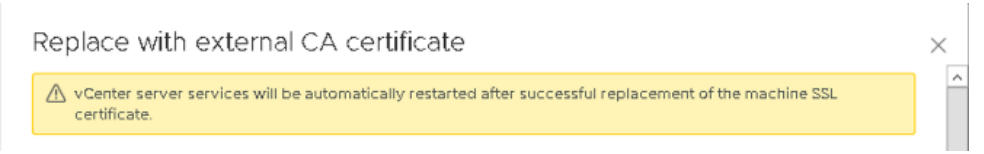
1. In the vSphere Client, on the **Certificate Management** page, select **SA-VCSA-01.VCLASS.LOCAL** from the **vCenter Server** drop-down menu.
2. Import and Replace the self-signed certificate.
   a. Under the Machine SSL Certificate card, select **Actions > Import and Replace Certificate**.

      The Replace Certificate wizard starts.

   b. On the Choose type of certificate to replace, select **Replace with certificate generated from vCenter server**.

   c. Click **NEXT**.

      A warning is placed in the interface for the user.



   d. Under the Machine SSL Certificate text box, click **BROWSE FILE**.

   e. From the folder `C:\Materials\Downloads`, select **machine_ssl.cer** and click **Open**.

      After selecting this file, the text box will be populated with the CA-signed certificate information.

   f. Under the Chain of trusted root certificates box, select **BROWSE FILE**.

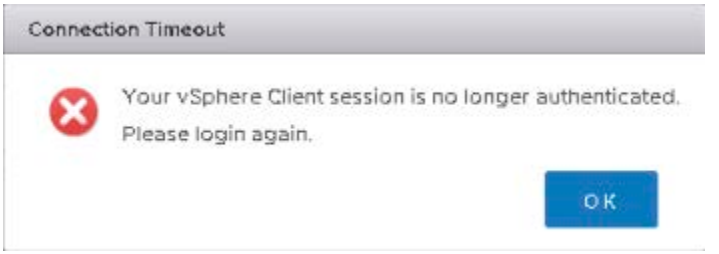
   g. From the folder `C:\Materials\Downloads`, select **root-64.cer** and click **Open**.

      After selecting this file, the text box will be populated with the root and chain certificate information.

h. On the Replace with external CA certificate page, click **REPLACE**.

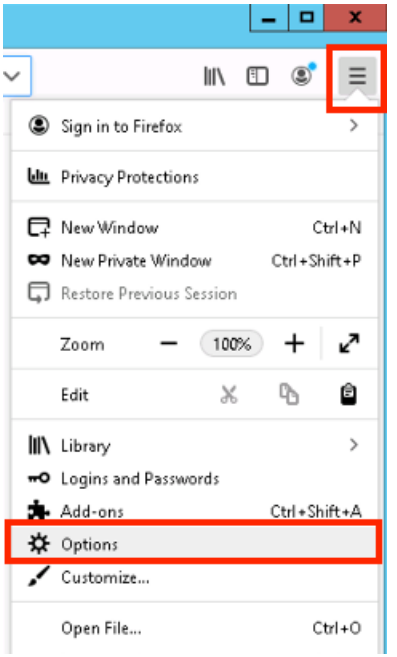
Shortly after the new CA-signed certificate import process successfully begins (in seconds), a message box indicating a connection timeout in the vSphere Client should display. This happens because replacing a security certificate causes vCenter Server services to restart including the vSphere Client UI.

You will need to restart the web browser to reconnect to the vSphere Client. You will do this at the end of the next step.



3. Clear the web cache and restart Firefox.

a. In a new Firefox tab, open the Firefox menu and select **Options**.



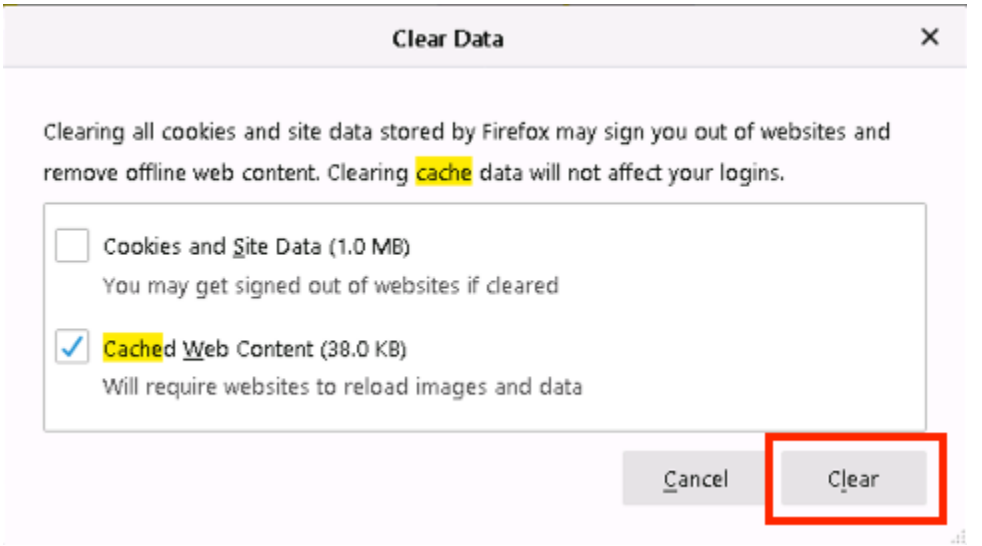
Alternatively, you can open a new Firefox browser tab and enter **`about:preferences`** in the Address box.

b. In the highlighted search box, search for **cache**.

c. Under Cookies and Site Data, select **Clear Data**.

d. In the Clear Data dialog box, deselect **Cookies and Site Data** and click **Clear**.

This action will clear the web cache of your Firefox browser.



e. Restart your Firefox browser.

4. Verify the certificate replacement.

After a longer wait (of at least 10 minutes), you must log back in to the vCenter Server instance because restarting the services ends the UI session.

a. Using the vSphere Client, log in to the vCenter Server sa-vcsa-01.vclass.local using your vCenter Server lab credentials.

b. If you get receive the security message `Warning: Potential Security Risk Ahead in your Firefox browser session`, click **Advanced...** and click **Accept the Risk and Continue** to proceed to the vCenter Server login page.

If you experience difficulties when attempting to log in to the vCenter Server instance in Site A, clear both Cached Web Content and Cookies and Site Data in the Firefox browser, then retry from step 4a.

If you cannot log in to vCenter Server after services have restarted, attempt to log in using a new private Firefox window.

c. Select **Menu > Administration** and select **Certificates > Certificate Management**.

d. On the Certificate Management page, select **SA-VCSA-01.VCLASS.LOCAL** from the vCenter Server **drop-down** list in the top-right of the pane.

e. Click **View Details** under Machine SSL Certificate.

f. Compare the valid dates and thumbprint information with the certificate information collected in task 1, step 6.

Valid from: _____
Valid until: _____

Thumbprint: _____

IMPORTANT

The valid dates and thumbprint of the current certificate should be different from the previous certificate.

The Valid from date should indicate today's date.

---

5. In the vSphere Client, select **Menu > Shortcuts.**

Lab 8 Configuring Identity Federation to Use Microsoft ADFS

Objective and Tasks

Configure vCenter Server identity provider federation with Microsoft ADFS:

1. Configure vCenter Server Identity Provider Federation
2. Add Permissions to vCenter Server for an AD Account
3. Log in to vCenter Server Using an AD Account

Task 1: Configure vCenter Server Identity Provider Federation

You configure vCenter Server to use Microsoft Active Directory Federation Services (ADFS).

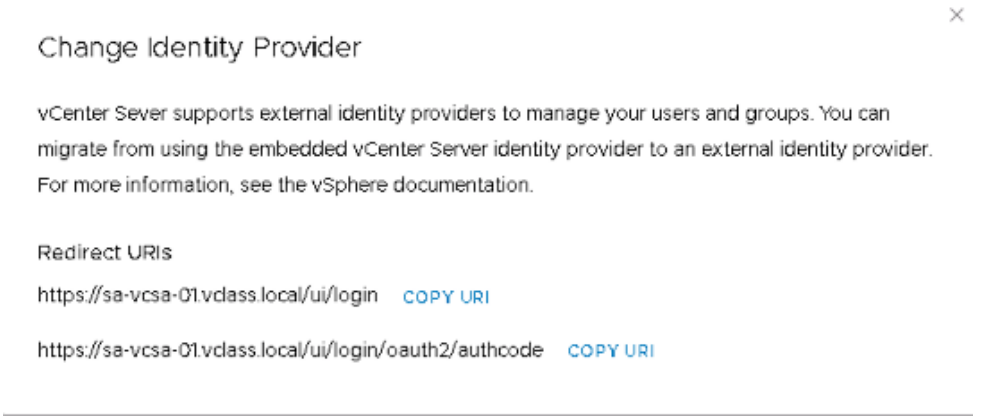
vCenter Server currently supports only ADFS as an external identity provider.

1. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar, and select **vSphere Client (SA-VCSA-01)**.
   a. If you are not logged in from a previous activity, log in using the vCenter Server lab credentials.
2. Select **Menu > Administration**.
3. In the left pane under Single Sign On, click **Configuration**.

   The **Identity Provider** tab appears in the right pane.

4. Obtain the redirect URI (Uniform Resource Identifier) links.

   a. In the **Identity Provider** tab, click the informational ("i") icon next to the **CHANGE IDENTIFY PROVIDER** link.



   b. Note the two URIs listed.

5. Click **CHANGE IDENTITY PROVIDER**.

   The Configure Main Identity Provider wizard appears.

6. On the Identity Provider page, leave **Microsoft ADFS** selected and click **NEXT**.

7. Configure the ADFS settings.

   a. On the student desktop, open the file **ADFS-Settings.txt** and review the ADFS configuration information.

   b. Return to the vSphere Client and the Configure Main Identity Provider wizard page.

   c. On the ADFS page, in the **Client Identifier** text box, enter the value for Client Identifier UID provided in the `ADFS-Settings.txt` file.

      Do not include any additional characters or spaces when you copy and paste the Client Identifier from the `ADFS-Settings.txt` file.

   d. In the **Shared secret** text box, enter the value for Client Secret provided in the `ADFS-Settings.txt` file.

      Do not include any additional characters or spaces when you copy and paste the Shared secret from the `ADFS-Settings.txt` file.

e. In the **OpenID Address** text box, enter the value for OpenID Address provided in the `ADFS-Settings.txt` file.

   Do not include any additional characters or spaces when you copy and paste the Shared secret from file ADFS-Settings.txt.

f. Click **NEXT.**

8. On the Users and Groups page, configure Active Directory (AD) over an LDAP connection.

   Avoid using any additional spaces in the entries for the AD LDAP configuration. These entry items are without spaces.

   a. In the **Base distinguished name for users** text box, enter **`cn=users,dc=vclass,dc=local`**.

   b. In the **Base distinguished name for groups** text box, enter **`dc=vclass,dc=local`**.

   c. In the **Username** text box, enter **`administrator@vclass.local`**.

   d. In the **Password** text box, enter **`VMware1!`**.

   e. In the **Primary server url** text box, enter **`ldaps://dc.vclass.local:636`**.

   f. Next to SSL certificates, click **BROWSE**.

   g. Double-click the **CAroot.cer** certificate file on the student desktop.

   h. Click **NEXT**.

9. Review the ADFS configuration and click **FINISH**.

10. Close Notepad++.

Task 2: Add Permissions to vCenter Server for an AD Account

You add permissions to vCenter Server for a user from the ADFS identity source.

1. Select **Menu > Hosts and Clusters**.
2. Add permissions to vCenter Server for the ADFS user.
   a. In the left pane, click **sa-vcsa-01.vclass.local**.
   b. Click the **Permissions** tab in the right pane.
   c. Click the **Add Permission** icon (the plus sign).

      The Add Permission window appears.
   d. Change the Domain to **Microsoft ADFS**.
   e. Next to User/Group, search for your ADFS account by entering **`Administrator`**.
   f. Leave the Administrator role selected.
   g. Select the **Propagate to children** check box.
   h. To finish adding the permissions for the ADFS user, click **OK**.

      You can monitor the task to completion in the Recent Tasks pane.
3. Verify that the permissions were added.
   a. On the **Permissions** tab, locate the newly added AD user MICROSOFT ADFS\Administrator.

      The vCenter Server role Administrator is indicated in the Role column.

      If you are able to find this entry, you are now ready to log in through the vSphere Client using Microsoft ADFS.
4. Log out of the vSphere Client.

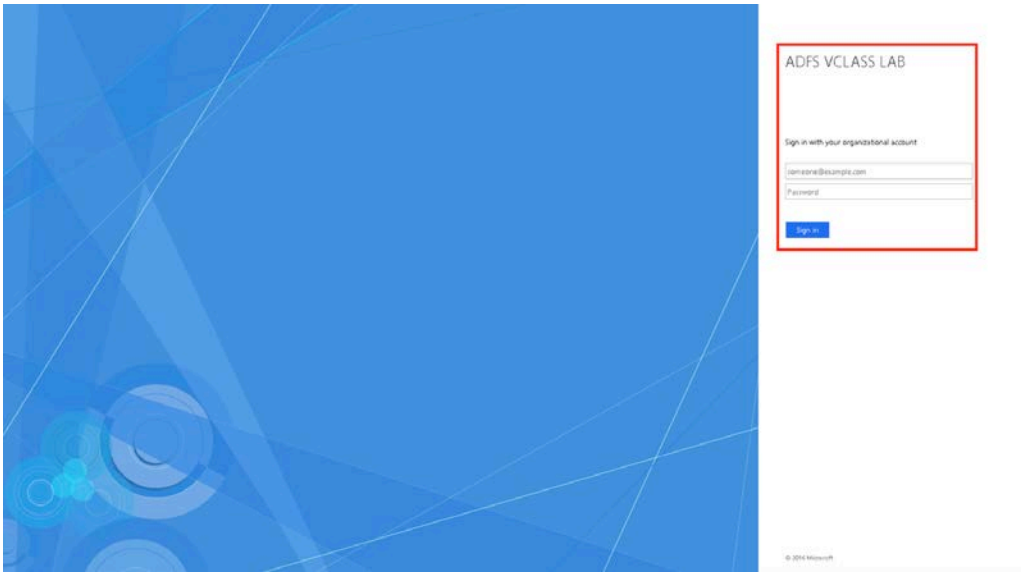
Task 3: Log In to vCenter Server Using an AD Account

You log in to vCenter Server as administrator@vclass.local, authenticated from your external identity provider Microsoft ADFS.

1. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar, and select **vSphere Client (SA-VCSA-01)**.

2. On the vSphere Client login page, enter **`administrator@vclass.local`** and click **NEXT**.

   After entering the Microsoft AD user name, you are automatically redirected to the identity provider login page.



3. On the identity provider login page, complete your login with Microsoft ADFS by entering user name **`administrator@vclass.local`** and password **`VMware1!`**.

   With permissions added to vCenter Server, you are allowed to log in.

   NOTE

   For Microsoft AD accounts which do not have permissions added to vCenter Server, login is not permitted even with correct AD credentials.

   ---

4. After successful login, log out of the vSphere Client and close Firefox.

Lab 9 Assigning a vSphere Trust Authority Administrator

Objective and Tasks

Assign a vSphere Trust Authority Administrator role to allow a user to configure and manage vSphere Trust Authority:

1. Assign a vSphere Trust Authority Administrator

Task 1: Assign a vSphere Trust Authority Administrator

You assign a vSphere Trust Authority administrator by adding a user to the TrustedAdmins Single Sign-On group.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. #In the vSphere Client, select **Menu > Administration**.
3. Select **Single Sign-On > Users and Groups**.
4. Select the **Groups** tab and select **TrustedAdmins**.
5. Click **ADD MEMBERS**.
6. In the search field, enter **`trustedadmin`** and select this user from the search results and click **SAVE**.
7. Confirm that the user trustedadmin@vsphere.local appears in the TrustedAdmins Single Sign-On group.

Lab 10 Enabling and Configuring vSphere Trust Authority

Objective and Tasks

Enable and configure vSphere Trust Authority:

1. Preconfigure the Environment
2. Export the TPM Certificate and ESXi Image Metadata
3. Export the Trusted User Principal
4. Enable vSphere Trust Authority Services
5. Import the Trusted Host Information to the Trust Authority Cluster
6. Create a Trusted Key Provider on the Trust Authority Cluster
7. Export the Trust Authority Cluster Settings
8. Import the Trust Authority Cluster Settings into the Trusted Hosts Cluster
9. Configure the Trusted Key Provider for the Trusted Hosts Cluster

Task 1: Preconfigure the Environment

You perform some preconfiguration in vCenter Server sites to facilitate the steps for vSphere Trust Authority configuration.

1. Log in to the vSphere Client on Site A.
    a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
    b. Select **vSphere Client (SA-VCSA-01)**.
    c. On the login page, enter the vCenter Server lab credentials.

       User name: **`administrator@vsphere.local`**
       Password: **`VMware1!`**

2. Rename the trusted (attested) cluster in Site A.
    a. In the vSphere Client, select **Menu > Hosts and Clusters**.
    b. Select **sa-vcsa-01.vclass.local** and expand the inventory object.
    c. Right-click **Trust-Authority-Cluster** and select **Rename...**.
    d. On the Rename page, enter **SA-Trusted-Cluster-01** and click **OK**.

       The trusted (attested) cluster is named and in Site A.
3. Rename the vSphere Trust Authority services cluster in Site B.
    a. In the vSphere Client, select **sb-vcsa-01.vclass.local** and expand the inventory object.
    b. Right-click **SB-Cluster** and select **Rename...**.
    c. On the Rename page, enter **SB-VTA-Cluster-01** and click **OK**.

       The cluster where vSphere Trust Authority services will run is named and in Site B.
4. Logout of the vSphere Client and minimize Firefox.

Task 2: Export the TPM Certificate and ESXi Image Metadata

You export the Trusted Platform Module (TPM) certificate and ESXi image metadata from the host to be attested.

IMPORTANT

Proceed slowly and methodically.

This lab is different. Almost all other labs take place using the vSphere Client whereas this lab and its tasks mostly take place at the PowerCLI command line.

When using PowerCLI in upcoming tasks, you will be:

- Connecting to the resource (Ensure that you use the correct user account to connect.)
- Performing configuration through the command line
- Disconnecting from the resource

Though you can type these commands out, using autocomplete for cmdlets at the PowerCLI command prompt, you can also copy and paste the PowerCLI commands in the vta.txt file.

---

1. On the Desktop, open the shortcut **Class Materials and Licenses** and open the **Downloads** folder.
2. Open the file **vta.txt** from this folder and resize the window for your use, as needed.

   This file contains all the PowerCLI commands which are required for the rest of this vSphere Trust Authority lab. You can copy and paste from this file instead of typing these commands by hand.
3. On the Desktop, double-click **Trust Authority** to open the PowerCLI window environment.
4. In PowerCLI, connect to the sa-esxi-08.vclass.local host that is to be attested, by using the root credentials.

   ```
   Connect-VIServer -server sa-esxi-08.vclass.local -User root
   -Password VMware1!
   ```
5. Assign the ESXi host to a variable.

   ```
   $vmhost = Get-VMHost
   ```
6. Inspect the TPM endorsement key of the ESXi host.

   ```
   Get-Tpm2EndorsementKey -VMHost $vmhost
   ```
7. Assign the TPM endorsement key to a variable.

   ```
   $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
   ```
8. Using the TPM endorsement key, export the TPM device CA certificate to the `C:\vta\` directory on the student desktop.

   ```
   Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath
   C:\vta\cacert.zip
   ```
9. Export the ESXi image metadata from the ESXi host.

   ```
   Export-VMHostImageDb -VMHost $vmhost -FilePath
   C:\vta\image.tgz
   ```
10. Disconnect existing PowerCLI sessions.

    ```
    Disconnect-VIServer -server * -Confirm:$false
    ```
11. Leave the PowerCLI session open.

Task 3: Export the Trusted User Principal

You export the trusted user principal from the vCenter Server system that manages the trusted (attested) cluster.

1. In PowerCLI, connect to the vCenter Server system that manages the trusted (attested) cluster by using the Trust Authority Administrator credentials.

   ```
   Connect-VIServer -server sa-vcsa-01.vclass.local -User
   trustedadmin@vsphere.local -Password VMware1!
   ```

2. Export the trusted user principal to the `C:\vta\` directory on the student desktop.

   ```
   Export-TrustedPrincipal -FilePath C:\vta\principal.json
   ```

3. Disconnect existing PowerCLI sessions.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   ```

4. Leave the PowerCLI session open.

Task 4: Enable vSphere Trust Authority Services

You enable vSphere Trust Authority services on the vSphere Trust Authority cluster.

1. In PowerCLI, connect to sb-vcsa-01.vclass.local by using the Trusted Administrator credentials.

   ```
   Connect-VIServer -server sb-vcsa-01.vclass.local -User
   trustedadmin@vsphere.local -Password VMware1!
   ```

2. Get the current Trusted Services state of the Trust Authority cluster.

   ```
   Get-TrustAuthorityCluster "SB-VTA-Cluster-01"
   ```

   NOTE

   The cluster reports the Trusted Services state as disabled.

3. Assign the current Trusted Services state of the Trust Authority cluster to a variable.

   ```
   $TAcluster = Get-TrustAuthorityCluster "SB-VTA-Cluster-01"
   ```

4. Enable Trusted Services on the Trust Authority cluster.

   ```
   Set-TrustAuthorityCluster -TrustAuthorityCluster $TAcluster
   -State Enabled
   ```

   a. To confirm enabling SB-VTA-Cluster-01, enter **Y**.

   NOTE

   The SB-VTA-Cluster-01 cluster is enabled as a vSphere Trust Authority services cluster. The services attestd and kmxd on the Trust Authority hosts have been started.

5. Verify that the cluster is set to Enabled.

   ```
   Get-TrustAuthorityCluster "SB-VTA-Cluster-01"
   ```

   When the cluster is enabled, the State column with show `Enabled`.

6. Disconnect the existing PowerCLI sessions.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   ```

7. Leave the PowerCLI session open.

Task 5: Import the Trusted Host Information to the Trust Authority Cluster

You import the trusted host information to the Trust Authority cluster.

1. In PowerCLI, connect to sb-vcsa-01.vclass.local by using the Trusted Administrator credentials.

   ```
   Connect-VIServer -server sb-vcsa-01.vclass.local -User
   trustedadmin@vsphere.local -Password VMware1!
   ```

2. In PowerCLI, import the trusted user principal from the trusted cluster into the Trust Authority cluster.

   ```
   New-TrustAuthorityPrincipal -TrustAuthorityCluster
   $TAcluster -FilePath C:\vta\principal.json
   ```

3. To verify that the previous import was successful, return the trusted user principal from the trusted cluster.

   ```
   Get-TrustAuthorityPrincipal -TrustAuthorityCluster
   $TAcluster
   ```

4. Import the TPM CA certificate from the trusted cluster into the Trust Authority cluster.

```
New-TrustAuthorityTpm2CACertificate -Name tpmca -
TrustAuthorityCluster $TAcluster -FilePath C:\vta\cacert.zip
```

NOTE

This step dictates which TPM devices are trusted by the Trust Authority cluster.

5. Import the ESXi image metadata from the trusted cluster into the Trust Authority cluster.

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster
$TAcluster -FilePath C:\vta\image.tgz
```

NOTE

This step dictates which versions of ESXi are trusted by the Trust Authority cluster.

6. Disconnect the existing PowerCLI sessions.

```
Disconnect-VIServer -server * -Confirm:$false
```

7. Leave the PowerCLI session open.

Task 6: Create a Trusted Key Provider on the Trust Authority Cluster

You create a trusted key provider on the Trust Authority cluster so that the Trust Authority cluster can request encryption keys from a key management server.

1. In PowerCLI, connect to sb-vcsa-01.vclass.local by using the Trusted Administrator credentials.

```
Connect-VIServer -server sb-vcsa-01.vclass.local -User
trustedadmin@vsphere.local -Password VMware1!
```

2. Add the key management server (KMS), called SB-KMS-01, as a Trust Authority key provider.

```
New-TrustAuthorityKeyProvider -TrustAuthorityCluster
$TAcluster -MasterKeyId 1 -Name SB-KMS-01 -KmipServerAddress
172.20.110.193
```

NOTE

The MasterKeyId is typically in the form of a longer UUID. In this lab, you use an internal PyKMIP KMS. This value differs depending on the KMS that is used. For more information, refer to the KMS vendor documentation.

---

3. Assign the key provider to a variable.

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$TAcluster
```

4. Create the trusted key provider client certificate.

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
$kp
```

5. Return the KMS certificate.

```
Get-TrustAuthorityKeyProviderServerCertificate -
KeyProviderServer $kp.KeyProviderServers
```

6. Assign the KMS certificate to a variable.

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -
KeyProviderServer $kp.KeyProviderServers
```

7. Add the KMS certificate to the trusted key provider in a trusted state.

```
Add-TrustAuthorityKeyProviderServerCertificate -
ServerCertificate $cert
```

8. Disconnect the existing PowerCLI sessions.

```
Disconnect-VIServer -server * -Confirm:$false
```

9. Leave the PowerCLI session open.

Task 7: Export the Trust Authority Cluster Settings

You export the settings for the Trust Authority cluster.

1. In PowerCLI, connect to sb-vcsa-01.vclass.local by using the Trusted Administrator credentials.

   ```
   Connect-VIServer -server sb-vcsa-01.vclass.local -User
   trustedadmin@vsphere.local -Password VMware1!
   ```

2. Export the Trust Authority Cluster information to the `C:\vta\` directory on the student desktop.

   ```
   Export-TrustAuthorityServicesInfo -TrustAuthorityCluster
   $TAcluster -FilePath C:\vta\cluster_settings.json
   ```

   NOTE

   This file contains information about the Trust Authority attestation services and key provider services.

3. Disconnect existing PowerCLI sessions.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   ```

4. Leave the PowerCLI session open.

Task 8: Import the Trust Authority Cluster Settings into the Trusted Hosts Cluster

You import the Trust Authority cluster settings into the trusted hosts cluster to establish a connection to the Trust Authority cluster.

1. Using PowerCLI, connect to the vCenter Server system that manages the trusted (attested) cluster.

   ```
   Connect-VIServer -server sa-vcsa-01.vclass.local -User
   trustedadmin@vsphere.local -Password VMware1!
   ```

2. Assign the trusted (attested) cluster to a variable.

   ```
   $TrustedCluster = Get-TrustedCluster "SA-Trusted-Cluster-01"
   ```

3. Import the Trust Authority cluster information.

   ```
   Import-TrustAuthorityServicesInfo -FilePath
   C:\vta\cluster_settings.json
   ```

   a. At the confirmation prompt, press Enter to accept the default (Y).

4. Enable the trusted cluster.

   ```
   Set-TrustedCluster -TrustedCluster $TrustedCluster -State
   Enabled
   ```

   a. At the confirmation prompt, press Enter to accept the default (Y).

5. Disconnect the existing PowerCLI sessions.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   ```

6. Close the Trust Authority command prompt window by entering **`exit`**.

Task 9: Configure the Trusted Key Provider for the Trusted Hosts Cluster

You configure the trusted key provider for the trusted (attested) cluster so that encryption keys can be received from the Trust Authority cluster.

1. Using the vSphere Client, connect to the vCenter Server **sa-vcsa-01.vclass.local**.

   a. Open a new tab in the Firefox web browser and navigate to **`https://sa-vcsa-01.vclass.local/ui`**.

   b. For the user name, enter **`trustedadmin@vsphere.local`**.

   c. For the password, enter **`VMware1!`**

2. Select **Menu** > **Hosts and Clusters**.

3. In the navigation pane, select **sa-vcsa-01.vclass.local**.

4. Click the **Configure** tab and select **Security > Key Providers**.

5. Click **ADD TRUSTED KEY PROVIDERS**.

   The trusted key providers that are available are shown with a Connected status.

6. Select **SB-KMS-01** and click **ADD KEY PROVIDERS**.

   The trusted key provider shows as Trusted and Connected. Because this is the first trusted key provider that you added, it is marked as the default.

   NOTE

   The trusted key provider becomes the default key provider for the entire vCenter Server system.

   If the Key Providers display does not indicate your Trusted Key Provider entry SB-KMS-01 and Connected status, stop and request assistance from your instructor.

7. Log out of the vSphere Client.

Lab 11 Encrypting a VM with a Trusted Key Provider

Objective and Tasks

Encrypt a VM with a trusted key provider:

1. Encrypt a VM with a Trusted Key Provider

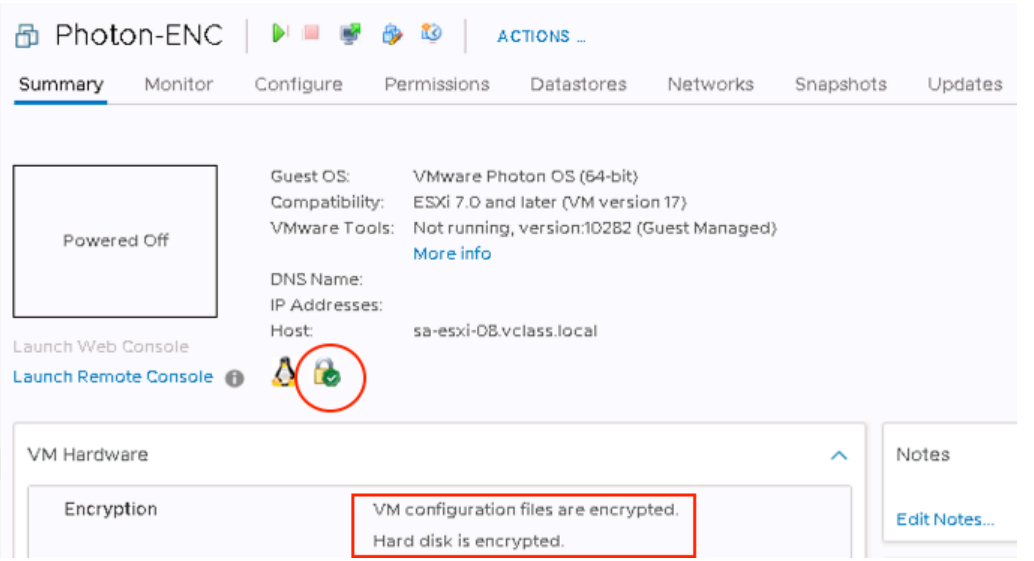
Task 1: Encrypt a VM with a Trusted Key Provider

You encrypt a VM with a trusted key provider so that the VM can only run on trusted hosts that are attested by the vSphere Trust Authority cluster.

1. Using the vSphere Client, connect to the vCenter Server instance **sa-vcsa-01.vclass.local.**
   a. Open a new Firefox tab and enter **`https://sa-vcsa-01.vclass.local/ui`** in the address bar.
   b. Enter user name **`trustedadmin@vsphere.local`**.
   c. Enter password **`VMware1!`**.
2. Select **Menu > Host and Clusters** to locate the VM **Photon-ENC** on the ESXi host sa-esxi-08.vclass.local.
   a. If the VM is powered on, shut it down by right-clicking the VM and selecting **Power > Shut Down Guest OS**.
3. Right-click **Photon-ENC** and select **VM Policies > Edit VM Storage Policies**.
4. From the **VM storage policy** drop-down menu, select **VM Encryption Policy**.

5. Click **OK**.

   The VM is encrypted with the configured trusted key provider.
   The VM summary displays a padlock icon with a green check mark to indicate that the VM is encrypted with a trusted key provider.



6. Power on the VM.
7. Logout of the vSphere Client.

Lab 12 Using Host Profiles

Objective and Tasks

Use host profiles to manage host configuration compliance:

1. Preconfigure ESXi Hosts
2. Create and Export a Host Profile
3. Import a Host Profile
4. Duplicate and Edit a Host Profile
5. Attach an ESXi Host to a Host Profile
6. Run an Initial Compliance Check
7. Introduce a Configuration Drift
8. Run a Compliance Check and Remediate the Configuration Drift
9. Detach the Host Profile

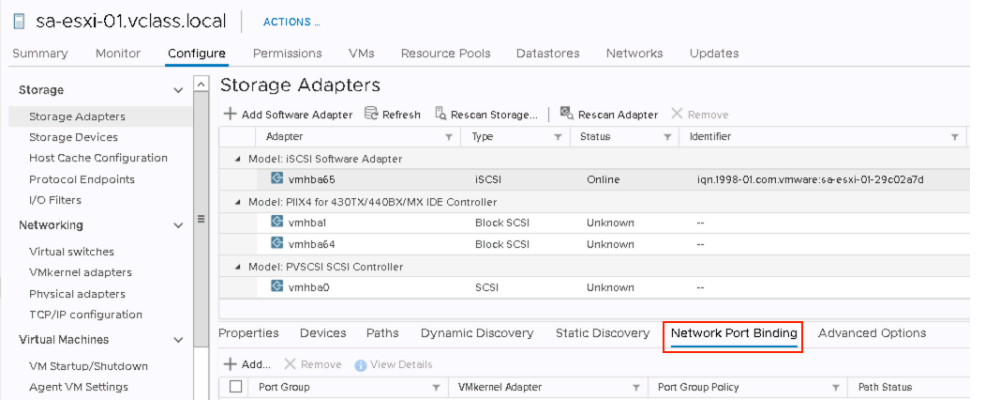
Task 1: Preconfigure ESXi Hosts

You use the vSphere Client to preconfigure an ESXi host.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**

2. Remove iSCSI network port binding from the sa-esxi-01.vclass.local host.
   a. In the vSphere Client, select **Menu > Hosts and Clusters**.
   b. In the navigation pane, click ESXi hosts **sa-esxi-01.vclass.local**.
   c. Select **Configure > Storage > Storage Adapters**.
   d. In the right pane under Model: iSCSI Software Adapter, select **vmhba65**.
   e. Select **Network Port Binding**.



   f. Select all items using the select all check box and click **Remove**.
   g. In the Remove All Active Paths dialog box, review the warning and click **OK**.

      A storage rescan is required because of a change in the storage configuration on the host.
   h. Under Storage Adapters, select **vmhba65** and click **Rescan Storage...**.
   i. In the Rescan Storage dialog box, accept the defaults and click **OK**.
   j. Monitor the task to completion.
3. Remove vmk1 from the sa-esxi-01.vclass.local host.
   a. In the vSphere Client, click **sa-esxi-01.vclass.local** on the left side.
   b. Select **Configure > Networking > VMkernel adapters**.
   c. In the right pane, select **vmk1** and click **Remove**.
   d. In the Remove VMkernel Adapter dialog box, review the information and click **REMOVE**.
   e. Monitor the task to completion.

4. Configure NTP on an ESXi host.
   a. Select **Menu > Hosts and Clusters**.
   b. In the left pane, select ESXi host **sa-esxi-02.vclass.local**.
   c. Select **Configure > System > Time Configuration**.
   d. In the right pane under Network Time Protocol settings, click **EDIT**.
   e. Change the NTP Servers setting to **1.2.3.4** and click **OK**.

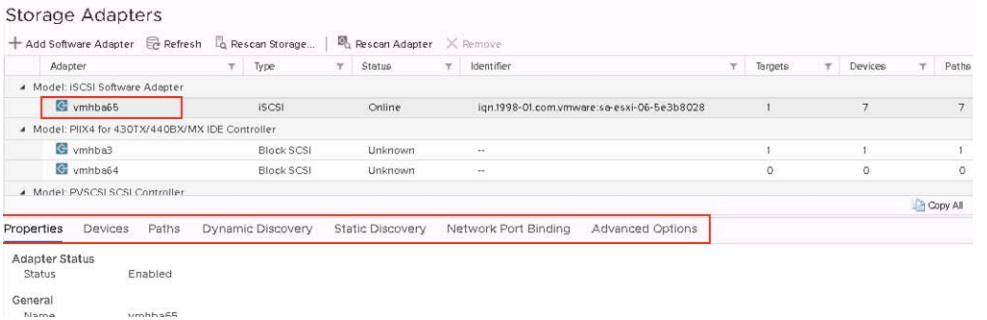
   IMPORTANT

   The NTP server for this host is being intentionally configured to an incorrect value for this lab exercise and will be corrected later on.

   ---

   f. Monitor the task to completion.
5. Add a software iSCSI adapter on the sa-esxi-02.vclass.local host.
   a. Select **Menu > Host and Clusters** and click **sa-esxi-02.vclass.local** in the left pane.
   b. In the right pane, select **Configure > Storage Adapters > +Add Software Adapter**.
   c. On the Add Software Adapter page, select **Add Software iSCSI adapter** and click **OK**.

      After the addition is complete, a new entry appears in the list of adapters in the right pane. You might need to scroll to locate vmhba65.
   d. In the right pane, click the **vmhba65** iSCSI software adapter and view the lower section of this pane update to display the software iSCSI adapter configuration.



   e. In the right pane, select **Dynamic Discovery**.
   f. Click **+Add...**.

g. On the Add Send Target Server page, enter **172.20.10.15** and click **OK**.

Whenever a storage change is made on a host or in a cluster, a rescan of attached storage is required.

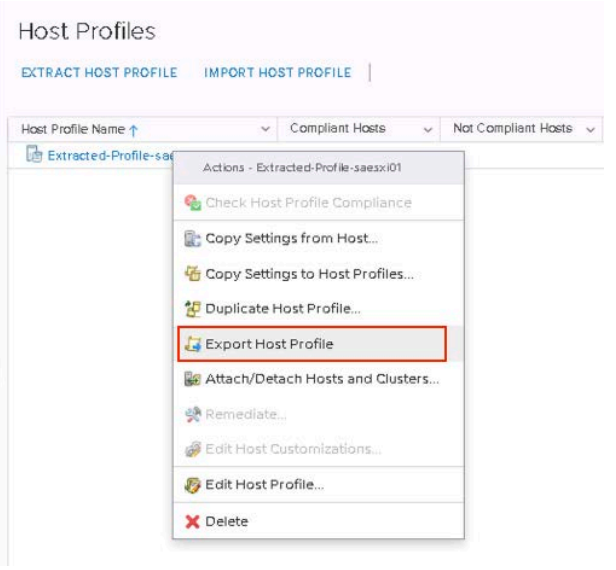
h. Select **vmhba65** under iSCSI Storage Adapter, click **Rescan Storage**, and click **OK**.

i. Monitor the task to completion.

Task 2: Create and Export a Host Profile

You create and export a host profile.

1. In the vSphere Client, select **Menu > Policies and Profiles**.
2. Select **Host Profiles** in the left pane and click **EXTRACT HOST PROFILE** in the right pane.
3. Extract a host profile.
   a. On the **Select host** page, select **sa-esxi-01.vclass.local** and click **NEXT**.
   b. On the Name and Description page, enter **Extracted-Profile-saesxi01** in the **Name** text box and click **FINISH**.
   c. In the Recent Tasks pane, monitor the task to completion.
4. Export the host profile to a file.
   a. In the right pane, right-click **Extracted-Profile-saesxi01** and select **Export Host Profile**.



b. In the Export Host Profile page, click **SAVE**.

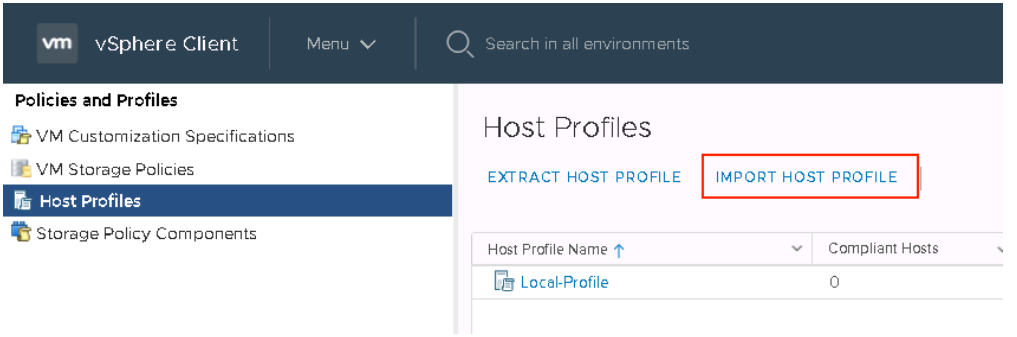
c. Save the profile as `Extracted-Profile-saesxi01_host_profile.vpf` on the desktop.

Task 3: Import a Host Profile

You import the host profile that you exported in the previous task.

Because host profiles do not store the reference host, host profiles can easily be imported and exported.

1. In the right panel, click the **Import Host Profile** icon.



2. In the Import Host Profile dialog box, import the host profile that you previously saved.

   a. On the Profile location line, click **Browse...**, select the file `Extracted-Profile-saesxi01_host_profile.vpf`, and click **Open**.

   b. In the **Name** text box, enter **`Imported-Profile-saesxi01`** and click **OK**.

   c. In the Recent Tasks pane, monitor the task to completion.

Task 4: Duplicate and Edit a Host Profile

You duplicate and edit the host profile that you imported in the previous task.

This editing process reduces the number of items checked for compliance through the profile on the ESXi host. This process also streamlines host configuration individually or in a cluster.

1. Duplicate a host profile.
    a. On the Host Profiles screen, select Imported-Profile-saesxi01 by clicking the horizontal row containing the profile name.
    b. Click **DUPLICATE HOST PROFILE**.
    c. On the Duplicate Host Profile page, enter **`Basic-Host-Configuration`** for the new profile name and click **OK**.
    d. On the Recent Tasks page, monitor the task to completion.
2. Edit a host profile.
    a. On the Host Profiles screen, select **Basic-Host-Configuration**.

    The profile currently contains all items/fields exported from the sa-esxi-01 host, by default.

    Because the host responsibilities and cluster membership might not be determined, some configuration items will be deselected from the host profile for compliance checking.

    b. Click **Configure** and click **EDIT HOST PROFILE...** on the right side.
    c. Deselect **Security and Services > Service Configuration**.
    d. Deselect **Storage configuration**.
    e. Click **SAVE**.

    Deselecting these items reduces the number of individual profile compliance checks for any attached host.

    f. In the Recent Tasks pane, monitor the task to completion.

Task 5: Attach an ESXi Host to a Host Profile

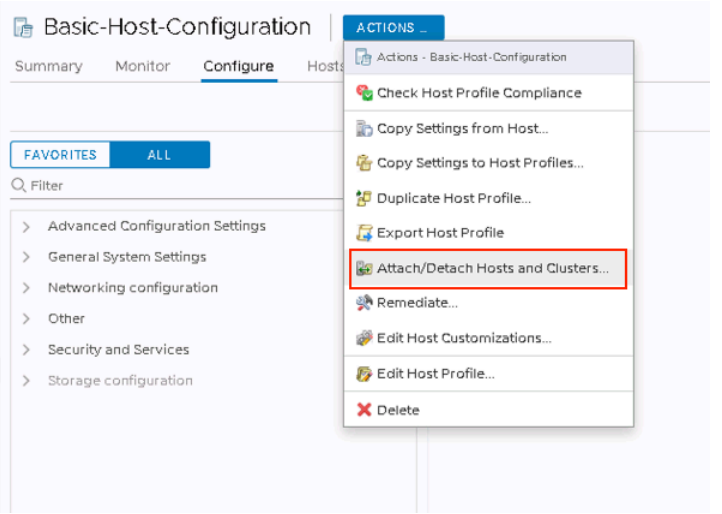
You attach an ESXi host or cluster to a host profile.

This profile has been edited and is based on the host profile that you previously imported.

Individual ESXi hosts and clusters can be attached or detached from a host profile in the Host Profile or the Host and Clusters view.

1. Select **Menu > Policies and Profiles**.
2. From the navigation pane, select **Host Profiles**.
3. In the right window pane, click **Basic-Host-Configuration** to navigate to that object.
4. In the right pane, click the **Configure** tab.

   You can review and edit the comprehensive list of configuration settings that define the host profile.
5. From the **Actions** drop-down menu, select **Attach/Detach Hosts and Clusters**.



   The Attach/Detach wizard appears.
6. Attach the host to the host profile.
   a. From the **Host/Cluster** list, select **sa-esxi-02.vclass.local** and click **SAVE**.
   b. In the Recent Tasks pane, monitor the task to completion.

Task 6: Run an Initial Compliance Check

You run a compliance check to verify the attached host configuration against all the settings that are specified by the host profile.

1. In the right pane, click the **Monitor** tab for the host profile.
2. Verify compliance for sa-esxi-02.vclass.local.
   a. Select **sa-esxi-02.vclass.local** and click **CHECK COMPLIANCE**.
   b. In the Recent Tasks pane, monitor the compliance check to completion.
3. Under the Host Profile Compliance column, click **Not Compliant** and view the compliance information near the middle of the screen.

   For greater visibility, minimize the Recent Tasks pane.

   The sa-esxi-02.vclass.local host is not compliant because the date and time configuration does not match the information in the host profile. The NTP server information is incorrect.
4. Resolve the date and time configuration issue occurring on the ESXi host.
   a. Click the **sa-esxi-02.vclass.local** host to transfer to the Host and Clusters view.
   b. In the right pane, select **Configure > System > Time Configuration** and click **EDIT** across from Network Time Protocol.
   c. In the NTP Servers box, enter **`172.20.10.10`** and click **OK**.

      Because this is the correct entry for the ESXi host configuration, it will match the host profile information.
   d. Select **Menu > Policies and Profiles**.
   e. In the left pane, select **Host Profiles**.

      Now that you have corrected the erroneous NTP Servers entry, it is time to check compliance.
   f. In the right pane, click **Basic-Host-Configuration**.
   g. Select **Monitor > Compliance**, select **sa-esxi-02.vclass.local**, and click **CHECK COMPLIANCE**.

      Monitor the task in the Recent Tasks pane to completion.
   h. The host is now compliant.

Task 7: Introduce a Configuration Drift

You test host profile compliance verification and remediation by introducing a noncompliant change on the host.

The noncompliant change is that you remove the vmnic2 adapter from the VDS dvs-Lab.

1. Select **Menu** > **Networking**.
2. In the left pane, expand **SA-Datacenter**, right-click distributed switch **dvs-Lab**, and select **Add and Manage Hosts**.

   The Add and Manage Hosts wizard appears.
3. On the Select task page, select **Manage host networking** and click **NEXT**.
4. On the Select hosts page, click **+Attached hosts**.
5. In the Select member hosts window, select the **sa-esxi-02.vclass.local**, click **OK**, and click **NEXT**.
6. On the Manage physical network adapters page, unassign the vmnic2 adapter.
   a. Under the sa-esxi-02.vclass.local host entry, expand this switch, select **vmnic2**, and record the attached uplink. _____
   b. Click **Unassign adapter** and click **NEXT**.
   c. In the Warning dialog box, review the information and click **OK**.
7. On the Manage VMkernel adapters page, click **NEXT**.
8. On the Migrate VM networking page, click **NEXT**.
9. On the Ready to complete page, review the selections and click **FINISH**.
10. In the Recent Tasks pane, monitor the task to completion.

Task 8: Run a Compliance Check and Remediate the Configuration Drift

You run a compliance check to detect noncompliant configuration changes that were made to hosts attached to a host profile. You then remediate the host.

1. Select **Menu** > Policies and Profiles.
2. In the left pane, click Host Profiles.
3. In the right pane, click Basic-Host-Configuration.
4. In the right pane, select Monitor > Compliance.
5. Select **sa-esxi-02.vclass.local** and click CHECK COMPLIANCE.

   In the Recent Tasks pane, monitor the compliance check to completion.
6. Click the **Not Compliant** entry for sa-esxi-02.vclass.local under the Host Profile Compliance column for additional details.
7. In the Compliance panel, review the compliance categories.

   Q1. How do the results of the compliance check differ from the compliance check performed in task 6?

   Q2. In the new category Virtual Network Setting, does the specific issue reported relate to the configuration change made in task 7?
8. Remediate the host.
   a. Select the **sa-esxi-02.vclass.local** host, click **EDIT HOST CUSTOMIZATIONS**, and **click OK**.

      With this customization step, you can review and edit information specific to the attached host.

   b. With the host selected, click PRE-CHECK REMEDIATION.

      The precheck remediation takes several moments to complete.

   c. Review the results of the pre-check remediation.

      This remediation action updates host settings to match those of the host profile that it is attached to.

      Q3. Will the host need to be put in maintenance mode?

      For the host to enter maintenance mode, the VMs on this host must be powered off or moved to another host.

      No VMs exist on this host.

d. Right-click the **sa-esxi-02.vclass.local** host and select **Maintenance Mode > Enter Maintenance Mode**.

   The Enter Maintenance Mode dialog box appears.

e. Review the information and click **OK**.

   The Host Profile window is updated to indicate that the host is `Ready to remediate`.

f. Select **sa-esxi-02.vclass.local** host and click **REMEDIATE**.

   The Remediate - Basic-Host-Configuration dialog box appears.

g. Review the information in the Remediate - Basic-Host-Configuration dialog box, accept the defaults, and click **OK**.

h. In the Recent Tasks pane, monitor the remediation and subsequent compliance check tasks to completion.

i. If the first host remediation attempt is unsuccessful, verify that the host is selected and attempt remediation again.

j. Verify that the host is now compliant.

9. Verify the action taken by host remediation.

   a. Select Menu > Networking.

   b. In the left pane, select the distributed switch dvs-Lab under SA-Datacenter.

   c. In the right pane, select Configure > Settings > Topology.

   d. From the left side of the topology diagram, click **pg-SA-Production** and expand **Uplink1** on the right side.

   e. Verify that remediation automatically reconnected vmnic2 on sa-esxi-02.vclass.local to the appropriate uplink Uplink1.

10. Return the host to production.

    a. Select **Menu > Host and Clusters**.

    b. Right-click **sa-esxi-02.vclass.local** and select **Maintenance Mode > Exit Maintenance Mode**.

    c. In the Recent Tasks pane, monitor the task to completion.

Task 9: Detach the Host Profile

Detach the host profile from the sa-esxi-02.vclass.local host.

1. Select **Menu** > **Policies and Profiles**.
2. In the left pane, click **Host Profiles**.
3. In the right pane, click **Basic-Host-Configuration**.
4. In the right pane, select **Actions > Attach/Detach Hosts and Clusters**.

   The Attach/Detach Hosts and Clusters wizard appears.
5. Detach the host from the host profile.
   a. In the **Host/Cluster** list, deselect **sa-esxi-02.vclass.local** and click **SAVE**.
   b. In the Recent Tasks pane, monitor the task to completion.
6. In the vSphere Client, select **Menu > Home**.

Lab 13 Creating Content Libraries

Objective and Tasks

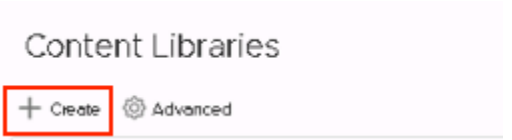
Create a multisite content library:

1. Create a Local Content Library
2. Upload Data to the Content Library
3. Create a Subscribed Content Library
4. Create a Subscription for VM Templates
5. Clone a Template to the Local Library
6. Synchronize the Content Libraries
7. Deploy a VM from the Subscribed Content Library
8. Clean Up for the Next Lab

Task 1: Create a Local Content Library

You create and configure a local content library that you publish externally for other content libraries to subscribe to.

1. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar, and select **vSphere Client (SA-VCSA-01)**.
   a. If you are not logged in from a previous activity, log in using the vCenter Server lab credentials.
2. In the vSphere Client, select **Menu > Content Libraries**.
3. Create a content library.
   a. In the right pane, click the **+Create** icon.



b. On the Name and location page, with vCenter Server sa-vcsa-01.vclass.local selected, enter **SA-Local-Library** in the **Name** text box and click **NEXT**.

c. On the Configure content library page, select **Local Content Library**.

d. Select **Enable publishing**.

e. Select **Enable authentication**.

f. In the **Password** and **Confirm password** text boxes, enter **VMware1!** and click **NEXT**.

g. On the Add storage page, click **OPSCALE-Datastore** and click **NEXT**.

h. On the Ready to complete page, confirm the information and click **FINISH**.

4. Monitor this task to completion in the Recent Tasks pane and verify that the SA-Local-Library content library appears in the list.

   a. If you do not see the new content library in the list, refresh the vSphere Client.

Task 2: Upload Data to the Content Library

You upload an Open Virtualization Format (OVF) file from your student desktop to the new content library.

1. In the right pane, right-click the **SA-Local-Library** library and select **Import Item**.
2. In the Import Library Item window, click **Local file** and click **UPLOAD FILES**.
3. In the File Upload window, click the **Desktop** icon in the left navigation panel.
4. Double-click the **Class Materials and Licenses** folder in the right pane and double-click the **Downloads** folder.
5. In the Downloads folder, double-click the **SampleVM** folder.
6. Double-click **SampleVM.ovf**.

   SampleVM.ovf is added to the Import Library Item dialog box. However, you must also upload **SampleVM-1.vmdk**, **SampleVM-2.iso**, and **SampleVM-3.nvram**.
7. Click the **UPLOAD** link to the right of SampleVM-1.vmdk.
8. In the File Upload window, select **SampleVM-1.vmdk**, press and hold the Ctrl key while selecting **SampleVM-2.iso** and **SampleVM-3.nvram**.

   You can use the Ctrl key to select multiple files in this window.

   Ensure that all three files are selected.
9. Release the Ctrl key and click **Open**.

   You should see four files ready to import before continuing.

10. Click **IMPORT**.
11. View the Recent Tasks pane to monitor the task to completion.

    The task takes some time to complete.
12. On the left pane, click **SA-Local-Library**.
13. In the right pane, click **Templates > OVF & OVA Templates.**
14. Verify that the uploaded SampleVM template is listed.

Task 3: Create a Subscribed Content Library

You configure a content library that is subscribed to the first library.

1. In the vSphere Client, select **Content Libraries** from the **Menu** drop-down menu.
2. Click the **SA-Local-Library** library in the left pane and click the **Summary** tab in the right window pane.
3. Copy the Subscription URL link for the SA-Local-Library content library to the clipboard.
   a. Scroll down until the Publication panel appears, and expand the panel if needed.
   b. Click **COPY LINK** to copy the Subscription URL in the Publication panel to the clipboard.
4. Select **Content Libraries** from the **Menu** drop-down menu.
5. In the right pane, click the **Create a new content library** (+) icon.

   The New Content Library wizard appears.
6. On the Name and location page, name the content library and verify the vCenter Server location.
   a. In the **Name** text box, enter **`SB-Subscribed-Library`**.
   b. Verify that **sb-vcsa-01.vclass.local** is selected in the **vCenter Server** drop-down menu.
   c. Click **NEXT**.
7. Configure a subscribed content library.
   a. Click **Subscribed content library**.
   b. Click the **Subscription URL** text box and press **`Ctrl+V`**.

      The subscription URL is pasted into the text box.

      If copy and pasting does not work, you must enter the URL manually.
   c. Select the **Enable authentication** check box.

d. In the **Password** text box, enter **VMware1!**.

e. In the Download content line, click **when needed** and click **NEXT.**

f. On the Add storage page, select **ESXi-01-Local** and click **NEXT**.

g. On the Ready to complete page, verify the selections and click **FINISH**.

h. View the Recent Tasks pane to monitor the task to completion.

8. View the contents of the content library subscriber.

   a. In the left pane, select the **SB-Subscribed-Library**.

   b. In the right pane, click the **Templates** tab.

   c. Under **Templates > OVF & OVA Templates**, verify that the SampleVM ovf template is present.

      This VM template is the same template that is in the source content library.

   d. Verify that the Stored Locally column indicates No and that the Size column indicates 0 bytes.

      The SB-Subscribed-Library library is configured to download library content only when needed. As a result, only the template's metadata has been synchronized. The actual template was not synchronized with the SB-Subscribed-Library library because it is not yet needed.

9. Turn off automatic synchronization.

   a. In the right pane, click the **Summary** tab.

   b. In the Subscription panel, click the **Edit Settings** link in the bottom-left panel corner.

   c. Under Automatic synchronization, deselect the **Enable automatic synchronization with the external content library** check box.

   d. Under the Password entry, enter the password that was used when creating the SB-Subscribed-Library library in the text box.

      The process fails if you do not enter the password.

   e. Select **Download library content only when needed**.

   f. Leave all other selections with their default settings and click **OK**.

   g. In the Subscription panel, verify that Automatic synchronization is now set to **off**.

Task 4: Create a Subscription for VM Templates

You create a subscription for VM Templates in the Local (Publisher) content library so that VM templates synchronize in the Subscriber library.

1. In the vSphere Client, select **Menu > Content Libraries**.
2. In the right pane, click **SA-Local-Library > Subscriptions** tab.
3. Create the subscription for the subscriber library.
   a. Click the **ACTIONS** drop-down menu and select **New Subscription...**.
   b. On the subscription type page, select **Create a new subscription to an existing Subscriber library** and click **NEXT**.
   c. On the Configure Subscription page, select **SB-VCSA-01.vclass.local**, select your **SB-Subscribed-Library** subscriber library, and click **NEXT**.
   d. On the Select folder page, select **SB-Datacenter** and click **NEXT**.
   e. On the Select compute resource page, select **sb-esxi-01.vclass.local** and click **NEXT**.
   f. On the Select Network page, select **VM Network** and click **NEXT**.
   g. On the Review page, verify your desired settings and click **FINISH**.
   h. Monitor the creation of the subscription under the Recent Tasks pane.

      If you do not see the subscription that you recently created in the list, repeat the steps in this task to completion.

Task 5: Clone a Template to the Local Library

You clone a VM template into the local content library.

1. Select **Menu > Hosts and Clusters**.
2. Clone a VM as a template to the local library.
   a. In the left pane, right-click the **Photon-01** VM and select **Clone** > **Clone as Template to Library**.

      The Clone Virtual Machine to Template window appears.
   b. On the Basic Information page, append **`-Library`** to the VM name in the **Name** text box and click **NEXT**.
   c. On the Location page, select **SA-Local-Library** and click **NEXT**.
   d. On the Select a compute resource page, select **sa-esxi-05.vclass.local** and click **NEXT**.

e. On the Select storage page, select **VM Storage Policy > Datastore Default**, select datastore **OPSCALE-Datastore**, and click **NEXT**.

f. On the Review page, verify your selections and click **FINISH**.

g. In the Recent Tasks pane, view the tasks that start up and monitor them to completion.

All tasks might take a few minutes to complete.

After the VM is cloned into Content Library, it becomes a managed VM template in vSphere 7.

3. View the VM template list in both libraries.

a. Select **Menu > Content Libraries**.

b. Observe the Local and Subscriber Content Library details.

Q1. How much storage space is being consumed in each library?

This value can be found under the Storage Used column on the Content Libraries list page.

Q2. How was the amount of storage used not the same between the libraries?

The local (publisher) and subscriber content libraries should have the same content.

Task 6: Synchronize the Content Libraries

You use the vSphere Client to synchronize the content libraries.

1. Synchronize VM templates between the libraries.

a. From the vSphere Client, select **Menu > Content Libraries**.

b. In the right pane, select **SA-Local-Library**.

c. Click the **Subscriptions** menu.

d. Select **SB-Subscribed-Library** selection and click **PUBLISH**.

e. In the Publish Library dialog box, click **PUBLISH**.

This action synchronizes the metadata between the libraries for the VM templates.

2. Verify that the metadata between the libraries is synchronized.

   a. Select **Menu > Content Libraries**.

   b. Observe both the templates column and the number of VM templates in each content library to verify that the metadata is synced.

      You might need to refresh the vSphere Client to see these numbers match.

      The SB-Subscribed-Library is only synchronizing metadata and not storage space. That is, the VM template and OVF items would need to be downloaded to the SB-Subscribed-Library to deploy VMs from them).

      Q1. How many VM templates now appear in the SB-Subscribed-Library content library?

Task 7: Deploy a VM from the Subscribed Content Library

You use the vSphere Client to deploy a new VM from the Photon-01-Library template that is available in the content library SB-Subscribed-Library.

To deploy a new VM from the subscriber library, you must first sync the VM template content from the published content library to the subscribed content library.

1. From the Content Libraries main page in the left pane, click **SA-Local-Library**.
2. In the right pane, click **Templates > VM Templates**.

   You should now be able to see the Photon-01-Library VM template that you previously cloned into the local library.

3. Right-click **Photon-01-Library** VM template and select **Publish**.

   The New Virtual Machine from Content Library wizard appears.

4. On the Publish Template page, select **SB-Subscribed-Library** and click **OK**.

   This step initiates a storage sync for this VM template from the local (publisher) library to the subscribed library.

   a. Monitor this task to completion using the Recent Tasks pane.

5. To verify the result, return to the Content Libraries main page (**Menu > Content Libraries**) and inspect the Storage Used column for the subscriber library.

   More than 400 MB of storage is now used in the subscribed library.

   After syncing the subscribed with the local library, you can now deploy a VM from the subscribed library.

6. From the Content Libraries main page in the left pane, select **SB-Subscribed-Library**.
7. In the right window, select **Templates > VM Templates**.

8. Deploy a VM from this VM template.
    a. Right-click the **Photon-01-Library** template and select **New VM from this Template...**.
    b. On the Deploy From VM template page, enter **`Photon-04`** in the **Specify a unique name and target location** text box and click **NEXT**.
    c. On the Select a compute resource page, under SB-Datacenter, select the **sb-esxi-01.vclass.local** host and click **NEXT**.
    d. On the Select storage page, select **ESXi-01-Local** and click **NEXT**.
    e. On the Select deploy options page, ensure that all check boxes are deselected and click **NEXT**.
    f. On the Ready to complete page, review your selections and click **FINISH**.
    g. In the Recent Tasks pane, view the tasks that started and monitor them to completion.

        All tasks might take a few minutes to complete.
9. Verify that the VM is deployed.
    a. Select **Menu > Hosts and Clusters**.
    b. In the left pane, verify that the Photon-04 VM appears in the inventory.

Task 8: Clean Up for the Next Lab

You shut down all VMs before continuing to the next lab.

1. Ensure that all VMs in the SA-Compute-01 cluster are shut down.
2. Select **Menu > Shortcuts**.

Lab 14 Managing Resource Pools

Objective and Tasks

Create and use resource pools:

1. Maintain VMs
2. Create CPU Contention
3. Create Resource Pools
4. Verify Resource Pool Functionality

Task 1: Maintain VMs

You rename one VM and then configure it and another VM to facilitate CPU contention.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. Select **Menu > Host and Clusters**.
3. Rename a VM.
   a. Expand **SA-Datacenter** and locate the sa-esxi-01.vclass.local host.
   b. In the Navigator pane, right-click the **WIN10-06** VM sad select **Rename**.
   c. Enter **`WIN10-03`** and click **OK**.

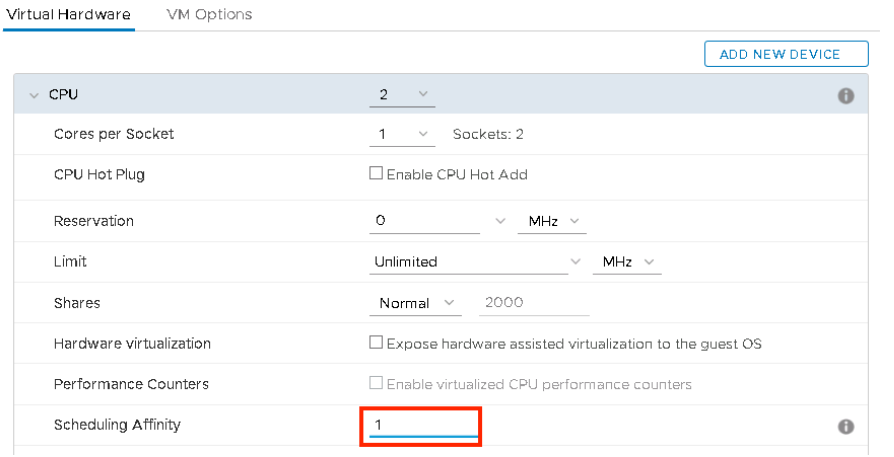
4. Configure the VM.

   a. In the Navigator pane, right-click the **Win10-02** virtual machine and select **Edit Settings**.

   b. On the **Virtual Hardware** tab, click the arrow next to **CPU**.

   c. In the **Scheduling Affinity** text box, enter **1**.

      This affinity setting forces the Win10-02 VM to run only on logical CPU 1.



CAUTION

CPU affinity is primarily used to create CPU contention for training purposes. VMware strongly discourages the use of this feature in a production environment.

   d. To apply these CPU configuration changes, click **OK**.

5. Change networking for the WIN10-02 VM.

   a. Right-click WIN10-02 and select **Edit Settings**.

   b. On the **Virtual Hardware** tab, locate Network Adapter 1 and select **Browse...** from the drop-down menu.

   c. On the Select Network page, select **pg-SA-Production** and click **OK**.

   d. Quickly verify your selection and, when ready, click **OK** to apply this networking change.

6. Repeat steps 4 and 5 for the Win10-03 VM.

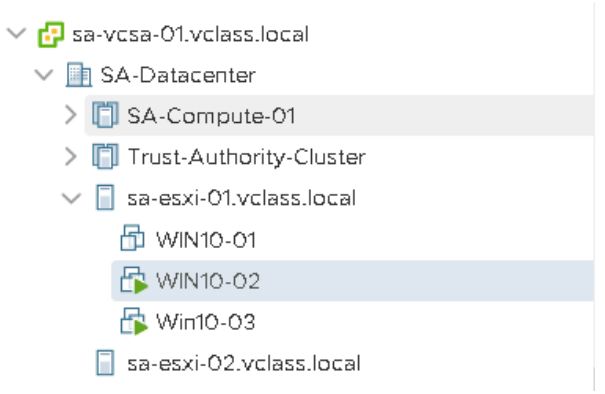
7. After preconfiguration is complete, power on VMs WIN10-02 and WIN10-03.

8. Return to the vSphere Client in the Firefox browser.

Task 2: Create CPU Contention

You use a tool to create CPU contention in your lab environment for testing. You force the VMs to compete for and share the limited logical CPU resources on the ESXi host, which might lead to performance degradation.

1. Select **Menu > Host and Clusters.**
2. Expand **SA-Datacenter**.
3. Verify that the WIN10-02 and WIN10-03 VMs are powered on and running on sa-esxi-01.vclass.local.



4. Start the CPUBUSY script on the VM desktops.
   a. Select **WIN10-02** in the left column.
   b. Select **Launch Web Console**.

      If you are asked to choose between VMRC and Web Console, choose the web console.

   c. On the desktop, right-click **CPUBUSY** and select **Open with Command Prompt**.

      This script runs continuously. It stabilizes in 1 to 2 minutes. This script repeatedly does floating-point computations. The script displays the duration (wall-clock time) of a computation, for example, `I did ten million sines in # seconds`.

   d. Repeat steps a through c on the WIN10-03 VM.

      You use the number of seconds reported as a performance estimate. The script CPUBUSY should run at approximately the same rate in each VM.
5. Leave the CPUBUSY script to run for 2 or more minutes to see contention.

Task 3: Create Resource Pools

You create resource pools to delegate control of a host's or a cluster's resources, and to compartmentalize all resources in a cluster.

1. Select **Menu > Host and Clusters**.
2. Right-click **sa-esxi-01.vclass.local** in the Navigator pane and select **New Resource Pool**.
3. Assign properties to the resource pool.

Option	Action
Name	Enter **`RP-Test`**.
CPU Shares	Select **Low** from the **Shares** drop-down menu.
All other settings	Leave the default settings.

4. Click **OK**.
5. In the Navigator pane, right-click **sa-esxi-01.vclass.local** and select **New Resource Pool**.
6. Assign properties to the resource pool.

Option	Action
Name	Enter **`RP-Production`**.
CPU Shares	Select **High** from the **Shares** drop-down menu.
All other settings	Leave the default settings.

7. Click **OK**.

Task 4: Verify Resource Pool Functionality

You assign VMs to resource pools with different resource settings to monitor and compare the performance differences.

1. Select the **RP-Test** resource pool in the Navigator pane and click the **Summary** tab.
2. Right-click **RP-Test > Edit Resource Settings** to inspect the number of shares in the RP-Test resource pool.

   Q1. What is the number of shares for this RP-Test (Low) resource pool?

3. Click **CANCEL**.
4. Select **RP-Production** in the Navigator pane and click the **Summary** tab.
5. Right-click **RP-Production > Edit Resource Settings** to inspect the number of shares in the RP-Production resource pool.

   Q2. What is the number of shares for this RP-Production (High) resource pool?

6. Click **CANCEL**.
7. Drag the **WIN10-02** VM to the **RP-Production** resource pool.
8. Drag the **WIN10-03** VM to the **RP-Test** resource pool.
9. Switch between VM consoles to monitor the results of the CPUBUSY script.
   a. Wait several minutes for CPU contention to occur.

      The contention should be evidenced on the WIN10-03 console by increased duration for the same executions. For example, calculations took 8 seconds before the VM was placed in the resource pool, and now it takes 32 seconds due to lower shares in the resource pool.

      Q3. What is the difference in performance between the two virtual machines?

10. In the vSphere Client, change the CPU shares of the RP-Test resource pool to **Normal**.
    a. Right-click the resource pool **RP-Test** in the Navigator pane and click **Edit Resource Settings**.
    b. From the **CPU > Shares** drop-down menu, select **Normal** and click **OK**.
    c. In each VM console, leave the script to run for a few minutes and compare the performance of the CPUBUSY script on each VM.

       As contention diminishes on the WIN10-03 VM, a difference in performance is noticeable.

11. Repeat the previous step to change CPU shares for the RP-Production resource pool to **Normal**.

    As contention diminishes, performance balances between the two VMs.

12. Press Ctrl+C in each Web Console window for VMs WIN10-02 and WIN10-03 to stop the CPUBUSY script.
13. Close the WIN10-02 and WIN10-03 web consoles.
14. Perform a graceful guest OS shutdown on VMs WIN10-02 and WIN10-03.
    a. In the navigation pane, right-click **WIN10-02** and select **Power> Shut Down Guest OS** selecting **YES** to confirm graceful Guest OS shutdown.
    b. In the navigation pane, right-click **WIN10-03** and select **Power> Shut Down Guest OS** selecting **YES** to confirm graceful Guest OS shutdown.
15. Click the VM graphic in the top-left corner of the vSphere Client.

Lab 15 Monitoring CPU Performance

Objective and Tasks

Use the `esxtop` command to monitor CPU performance:

1. Run a Single-Threaded Program in a Single-vCPU VM
2. Start esxtop and View Statistics
3. Record Statistics for Case 1: Single Thread and Single vCPU
4. Run a Single-Threaded Program in a Dual-vCPU VM
5. Record Statistics for Case 2: One Thread and Two vCPUs
6. Run a Dual-Threaded Program in a Dual-vCPU VM
7. Record Statistics for Case 3: Two Threads and Two vCPUs
8. Analyze the Test Results

Task 1: Run a Single-Threaded Program in a Single-vCPU VM

You run a test program to generate continuous database activity on the test VM for statistical analysis.

The test VM is configured with one vCPU.

1. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar, and select **vSphere Client (SA-VCSA-01)**.
    a. If you are not logged in from a previous activity, log in using the vCenter Server lab credentials.
2. Select **Hosts and Clusters** from the **Menu** drop-down menu.
3. In the left pane, expand **SA-Datacenter** and expand the **SA-Compute-01** cluster.

4. Verify that the Linux01 VM is hosted on sa-esxi-04.vclass.local.
   a. In the left pane, expand the inventory and select **Linux01**.
   b. In the right pane, view the **Summary** tab and verify that the host on which Linux01 resides is sa-esxi-04.vclass.local.
5. Power on the virtual machine Linux01 VM.
6. Log in to the virtual machine Linux01 web console.
   a. On the **Summary** tab, click the **Launch Web Console** link.
   b. Wait for the VM to complete its boot process.
   c. Log in by entering username **`root`** and password **`VMware1!`**.
7. Verify that you are in the `/root` directory.

   ```
   pwd
   ```

8. If you are not in the `/root` directory, change to the root directory.

   ```
   cd /root
   ```

9. Start the test program on Linux01.

   ```
   ./starttest1
   ```

   The test program generates database operations to a medium-size database and writes output to the screen. The program must run uninterrupted.

Task 2: Start esxtop and View Statistics

You use the `esxtop` command to observe performance statistics for supported objects.

1. Start an SSH session to sa-esxi-01.vclass.local.
   a. On the student desktop taskbar, click the **MTPuTTY** shortcut.
   b. In the Servers pane on the left, double-click **SA-ESXi-04**.
   c. If the PuTTY security alert appears, click **Yes**.

      You are automatically logged in to the appliance as username root.
2. Start the real-time monitoring program esxtop.

   ```
   esxtop
   ```

   By default, `esxtop` starts with the CPU screen.

3. Change the update delay from the default 5 seconds to 10 seconds.
   a. Enter **s**.
   b. Enter **10**.
4. Filter the CPU screen output to display only VMs by pressing Shift+v.

   By default, the CPU screen shows statistics for VM processes and active ESXi host processes.
5. In the output table, find the Linux01 VM statistics.

Task 3: Record Statistics for Case 1: Single Thread and Single vCPU

You record statistics for the first test case.

1. After 30 seconds of statistics collection, record the values for the Linux01 VM in the Case 1 column in the class configuration handout.
   - %USED
   - %RDY
   - %IDLE
2. Record the operations per minute (OPM) value in the test script.
   a. In Firefox, click the **Linux01** console tab.
   b. Record the OPM value reported by the test script in the Case 1 column in the class configuration handout.

      The counter value is reported with each iteration that the test script performs. Use the counter reported in the last iteration.
3. Press Ctrl+C to stop the test script.
4. Close the **Linux01** web console.

Task 4: Run a Single-Threaded Program in a Dual-vCPU VM

You modify the Linux01 VM to have two vCPUs and you restart the test script.

1. From the vSphere Client, shut down the Linux01 VM.
2. Wait for the running indicator to be removed from the Linux01 VM icon in the inventory tree.

   You might need to click the **Refresh** icon.
3. Add a second vCPU to the Linux01 VM.
   a. In the left pane, right-click **Linux01** and select **Edit Settings**.
   b. On the **Virtual Hardware** tab in the Edit Settings dialog box, select **2** from the **CPU** drop-down menu and click **OK**.
   c. In the Recent Tasks pane, monitor the reconfiguration task to completion.
4. Power on the Linux01 VM.
5. On the **Summary** tab, click the **Launch Web Console** link.
6. Wait for the VM to complete its boot process.
7. Log in by entering username **`root`** and password **`VMware1!`**.
8. On the **Linux01** console tab, restart the test program from the directory `/root.`

   `./starttest1`

   This script generates database operations to a medium-size database. The number of threads is set to **1**. The script must run uninterrupted.

Task 5: Record Statistics for Case 2: One Thread and Two vCPUs

You record statistics for the second test case.

1. Record the `esxtop` counter values.
   a. Change to the MTPuTTY window.
   b. Enter **e**.
   c. Enter the GID for Linux01.
   d. Examine the two lines in the NAME column that start with vmx-vcpu.

      These two lines show the activity of each of the vCPUs in the Linux01 VM.
   e. After 30 seconds of statistics collection, record the values for vCPU0 and vCPU1 in the Case 2 column in the class configuration handout.
      - %USED
      - %RDY
      - %IDLE
2. Record the OPM value in the test script.
   a. In Firefox, click the **Linux01** console tab.
   b. Record the OPM value reported by the test script in the Case 2 column in the class configuration handout.

      The counter value is reported with each iteration that the test script performs. Use the counter reported in the last iteration.
3. Press **Ctrl+C** to stop the test script in the Web Console session to Linux01.

Task 6: Run a Dual-Threaded Program in a Dual-vCPU VM

You configure the third case parameters by running a two-threaded test program on a VM with two vCPUs.

1. On the **Linux01** console tab, start the two-threaded test program.

   ```
   ./starttest2
   ```

   This script generates database operations to a medium-size database. The number of threads is set to 2. The script must run uninterrupted.

Task 7: Record Statistics for Case 3: Two Threads and Two vCPUs

You record statistics for the final test case.

1. Record the `esxtop` counter values.
   a. Change to the MTPuTTY window.
   b. Examine the two lines in the NAME column that start with vmx-vcpu.

      These two lines show the activity of each of the vCPUs in the Linux01 VM.

   c. After 30 seconds of statistics collection, record the values for vCPU0 and vCPU1 in the Case 3 column in the class configuration handout.
      - %USED
      - %RDY
      - %IDLE
2. Record the OPM value in the test script.
   a. In Firefox, click the **Linux01** console tab.
   b. Record the OPM value reported by the test script in the Case 3 column in the class configuration handout.
3. Press **`Ctrl+C`** to stop the test script in the Web Console session to Linux01.
4. Stop the `esxtop` program.
   a. Change to the MTPuTTY window.
   b. Enter **`q`** to stop `esxtop`.
5. Keep the SA-ESXi-04 MTPuTTY session open for the next lab.
6. Keep the **Linux01** console tab open for the next lab.
7. Keep the **vSphere Client** open for the next lab.

Task 8: Analyze the Test Results

You analyze the captured statistics and document your conclusions.

1. Review the statistics that you recorded in the class configuration handout in tasks 3, 5, and 7.
2. Record conclusions that you can draw from the data in the class configuration handout.

Lab 16 Monitoring Memory Performance

Objective and Tasks

Use the `esxtop` command to monitor memory performance under load:

1. Generate Database Activity in the Test VM
2. Check for Overcommitment of VM Memory
3. Configure esxtop to Report VM Memory Statistics
4. Observe Memory Statistics
5. Start a Memory Test on ResourceHog01 and ResourceHog02
6. Record Memory Statistics
7. Clean Up for the Next Lab

Task 1: Generate Database Activity in the Test VM

You start the test program to generate database activity.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. Select **Menu > Hosts and Clusters.**
3. In Firefox, click the **Linux01** console tab.

4. If necessary, log in to the Linux01 VM as user **root** and the standard lab password.
5. In the Linux01 console, start the test script `starttest2` from the folder `/root` in Linux01 VM.

   ```
   ./starttest2
   ```

   This test program performs continuous database operations to a medium-size database. The number of threads is set to 2. The script must run uninterrupted.

Task 2: Check for Overcommitment of VM Memory

You use resource allocation reports to determine whether memory is overcommitted for a VM.

1. Using the vSphere Client, select **Menu > Hosts and Clusters.**
2. In the left pane, select the **Linux01** VM.
3. In the right pane, click the **Monitor** tab and click **Utilization** on the left.
4. Find the Virtual Machine Memory panel.
5. Record the value for VM Consumed. _____
6. Find the Guest Memory panel in the lower-left corner of the right pane.
7. Record the value for Active Guest Memory. _____

   Q1. Is the consumed host memory greater than the active guest memory?

   If the consumed host memory is greater than the active guest memory, memory is not overcommitted. If the consumed host memory is less than active guest memory, then overcommitment is occurring and might cause degraded performance.

Task 3: Configure esxtop to Report VM Memory Statistics

You start `esxtop` and configure it for memory statistics.

1. Open the MTPuTTY window to monitor statistics for the VM on the host.
   a. From the student desktop, click the **MTPuTTY** shortcut on the taskbar.
   b. In the Servers pane on the left, double-click **SA-ESXi-04**.
   c. When the MTPuTTY security alert appears, click **Yes**.

      You are automatically logged in to sa-esxi-04.vclass.local as user root.
2. Start `esxtop`.
3. In `esxtop`, enter **m** to view the memory statistics screen.

4. Set a 10-second update delay.
    a. Enter **s** to display the delay prompt.
    b. At the delay prompt, enter **10**.
5. To display only VM statistics, enter **Shift+v** .
6. Remove all statistics columns from the output table, except D, H, J, and K.

    Removing counters that are not monitored during the test can make isolation of the desired counters easier.
    a. Enter **f** to access the field order screen.
    b. If an asterisk appears to the left of the field name, for fields other than D, H, J, and K, press the corresponding letter to remove the asterisk.
    c. If an asterisk does not appear to the left of the field name, for the D, H, J, and K fields, press the corresponding letter to add an asterisk.
    d. Press **Enter** to return to the memory statistics output.

Task 4: Observe Memory Statistics

You observe `esxtop` counters to determine memory conditions.

1. Examine `esxtop` statistics.
    a. In the `esxtop` output, view the Linux01 VM statistics.
    b. To change the view to the memory view, enter **m**
    c. Verify that the MCTLSZ, MCTLTGT, SWCUR, SWTGT, SWR/s, and SWW/s values are at or near zero.
    d. If you cannot see all values listed in step b, close the left pane in the MTPuTTY application - collapsing the Servers list in MTPuTTY.
2. Record the operations per minute (OPM) value in the test script.

    The counter value is reported with each iteration that the test script performs. Use the counter reported in the last iteration.
    a. Change to the **Linux01** console tab.
    b. Record the OPM value reported by the test script. _____

        The counter value is reported with each iteration that the test script performs. Use the counter reported in the last iteration.

Task 5: Start a Memory Test on ResourceHog01 and ResourceHog02

You start a memory test on the ResourceHog01 and ResourceHog02 VMs.

1. Power on and monitor VM ResourceHog01.

   You must enter the console within 30 seconds.

   a. Return to the **vSphere Client** tab.

   b. In the left pane, select **ResourceHog01**.

   c. If it is not there already, **migrate** ResourceHog01 VM to host **sa-esxi-04.vclass.local**.

   NOTE

   Keep all VMs for this exercise on sa-esxi-04.vclass.local.

   ---

   d. Right-click **ResourceHog01** and select **Power** > **Power On**.

   e. Click the **Summary** tab of ResourceHog01 and click the **Launch Web Console** link.

   f. Click anywhere in the console window.

   g. At the BIOS screen, press **Enter**.

   h. At the `boot:` prompt, press Enter to load the Ultimate Boot CD menu.

      If you see a `Booting...` prompt, you did not enter the console within 30 seconds. You must restart the process from substep a and enter the console to the VM within 30 seconds. Repeat this process until the Ultimate Boot CD menu appears.

   i. Use the arrow keys and the Enter/Return key to select **Mainboard Tools** > **Memory Tests > Memtest86+ V1.70**.

      The exact keystroke sequence is Enter, down arrow, down arrow, Enter, down arrow, down arrow, Enter.

   j. After the memory test utility is running, press Ctrl+Alt to release the pointer focus.

2. Repeat step 1 for the ResourceHog02 VM.

Task 6: Record Memory Statistics

You record and evaluate memory statistics with a significant load consuming ESXi host memory.

1. Return to the MTPuTTY window.
2. After at least one minute of statistics collection, record the values for the ResourceHog02, ResourceHog01, and Linux01 VMs in the class configuration handout.
   - MCTL?
   - MCTLSZ
   - MCTLTGT
   - SWCUR
   - SWTGT
   - SWR/s
   - SWW/s
   - %SWPWT

   Q1. For Linux01, does the value of MCTLSZ converge with the value of MCTLTGT?

   Q2. For Linux01, does the value of SWCUR converge with the value of SWTGT?
3. Monitor the statistics output until the host reaches a steady state where the counters in each set are close in value to each other.

   If the counters in each set are close in value to each other, the host has reached a steady state.
4. To determine which VMs do not have the balloon driver installed, examine the **MCTL?** value for each VM.

   The MCTL? field indicates the presence of the balloon driver. If the **MCTL?** value is Y, then that VM has a balloon driver installed. Otherwise, the VM lacks a balloon driver.

   Q3. Which VMs do not have the balloon driver installed?
5. To determine whether the VMs are swapping, examine the values for SWR/s and SWW/s for each VM.

   Q4. Which VMs are swapping?
6. Determine which VMs have experienced degraded performance as a result of swapping.
   a. Enter lowercase **c** to change to the CPU screen.
   b. Press Shift+V to display only VM statistics.

c. Examine the %SWPWT value for each VM identified as actively swapping.

%SWPWT is the percentage of time the world is waiting for the ESX VMkernel swapping memory. As %SWPWT exceeds 5 percent, the performance of the VM degrades significantly. If you do not see the %SWPWT field, expand your console window.

Q5. What are the %SWPWT values for each of the VMs?

7. Enter **m** to return to the `esxtop` memory screen.

The memory state can be found at the end of the third row from the top of the `esxtop` output.

Q6. What is the memory state: high, clear, soft, hard, or low?

8. Record the OPM value in the test script.

a. Change to the **Linux01** console tab.

b. Record the OPM value reported by the test script. _____

c. Compare this OPM value with the value that you recorded in task 4 (step 2, substep b).

Q7. Has the performance of the test script degraded?

Task 7: Clean Up for the Next Lab

You stop the test script on the Linux01 VM. You also stop the memory tests on the ResourceHog01 and ResourceHog02 VMs.

1. In the MTPuTTY window, select **View** > **Servers** to display the Servers pane on the left.
2. Keep `esxtop` running in the MTPuTTY window.
3. Change to the **Linux01** web console tab and press Ctrl+C to stop the test script.

Keep the console tab open.

4. Close the **ResourceHog01** and **ResourceHog02** console tabs.
5. **Power off** the ResourceHog01 and ResourceHog02 VMs.
6. Select **Menu > Home**.

Lab 17 Monitoring Storage Performance

Objective and Tasks

Use the `esxtop` command to monitor disk performance across a series of tests:

1. Prepare to Run Tests
2. Measure Continuous Sequential Write Activity to a Virtual Disk on a Remote Datastore
3. Measure Continuous Random Write Activity to a Virtual Disk on a Remote Datastore
4. Measure Continuous Random Read Activity to a Virtual Disk on a Remote Datastore
5. Measure Continuous Random Read Activity to a Virtual Disk on a Local Datastore
6. Analyze the Test Results

Task 1: Prepare to Run Tests

You use several test scripts on the Linux01 VM to generate continuous random and sequential I/O operations against both local and remote (network) datastores. You monitor storage preparation tasks to completion and change folders.

The Linux01 VM is on sa-esxi-04.vclass.local and is configured with two hard drives to serve as local and remote I/O targets. One SCSI drive is stored on the 11GBLocal local datastore and the other SCSI drive is stored on the 11GBRemote remote datastore.

1. Log in to the vSphere Client on Site A.
    a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
    b. Select **vSphere Client (SA-VCSA-01)**.
    c. On the login page, enter the vCenter Server lab credentials.

    User name: **`administrator@vsphere.local`**
    Password: **`VMware1!`**

2. In Firefox, click the **Linux01** web console tab.

   a. If necessary, log in by entering user name **root** and password **VMware1!**.

3. Run a script from the `/root` directory on the Linux01 VM to configure storage.

   ```
   ./storageconfig.sh
   ```

   The storage preparation might take a few minutes to finish. The script must run uninterrupted to completion.

4. When the script is finished, navigate to the test scripts folder.

   ```
   cd aio-stress
   ```

Task 2: Measure Continuous Sequential Write Activity to a Virtual Disk on a Remote Datastore

You run the `logwrite.sh` test script to generate continuous sequential write activity to the hard disk on the remote datastore.

1. In the Linux01 web console, run the test script uninterrupted.

   ```
   ./logwrite.sh
   ```

2. View the MTPuTTY session to the sa-esxi-04 host.

   MTPuTTY should be logged in to SA-ESXi-04 and `esxtop` should be running.

3. If you are not logged in to MTPuTTY and `esxtop` is not running, start a new MTPuTTY session to the SA-ESXi-04 host.

   a. In MTPuTTY, open a connection to SA-ESXi-04.

   b. Enter **esxtop** at the command prompt.

   c. Set the screen refresh to 10 seconds by entering **s** and then entering **10**.

4. Enter **d** to display device adapter output and examine the reads and writes to the adapter paths.

   Q1. Which adapter has the most disk I/O activity?

5. Enter **u** to display individual device output and examine the reads and writes to the devices.

   One of the remote devices has more disk I/O activity than the others.

6. Enter **v** to display the VM output.
7. After 30 seconds of statistics collection, record the values for the Linux01 VM.

   The values can be recorded in the Sequential Writes/Remote Datastore column in the class configuration handout.

   - READS/s
   - WRITES/s
8. In Firefox, click the **Linux01** web console tab.
9. To stop the test script running, press **Ctrl+C**.

Task 3: Measure Continuous Random Write Activity to a Virtual Disk on a Remote Datastore

You run the `datawrite.sh` test script to generate continuous random write activity to the VM hard disk on the remote datastore.

1. In the Linux01 web console, start the test script and let it run uninterrupted.

   ```
   ./datawrite.sh
   ```
2. Return to the MTPuTTY window.
3. Enter **d** to display device adapter output and examine the reads and writes to the adapter paths.
4. Enter **u** to display individual device output and examine the reads and writes to the devices.
5. Enter **v** to display the VM output.
6. After 30 seconds of statistics collection, record the values for the Linux01 VM.

   The values can be recorded in the Random Writes/Remote Datastore column in the class configuration handout.

   - READS/s
   - WRITES/s
7. In Firefox, select the **Linux01** web console tab.
8. To stop the test script, press **Ctrl+C**.

Task 4: Measure Continuous Random Read Activity to a Virtual Disk on a Remote Datastore

You run the `fileserver2.sh` test script to generate continuous random read activity from the hard disk on the remote datastore.

1. In the Linux01 web console, start the test script and let it run uninterrupted.

   `./fileserver2.sh`

2. Return to the MTPuTTY window.
3. Enter **d** to display device adapter output and examine the reads and writes to the adapter paths.
4. Enter **u** to display individual device output and examine the reads and writes to the devices.
5. Enter **v** to display the VM output.
6. After 30 seconds of statistics collection, record the values for Linux01 VM.

   The values can be recorded in the Random Reads/Remote Datastore column in the class configuration handout.

   - READS/s
   - WRITES/s

7. In Firefox, select the **Linux01** web console tab.
8. To stop the test script, press **`Ctrl+C`**.

Task 5: Measure Continuous Random Read Activity to a Virtual Disk on a Local Datastore

You run the `fileserver1.sh` test script to generate continuous random read activity from the VM hard disk on the local datastore attached to the ESXi host.

1. In the Linux01 web console, start the test script and let it run uninterrupted.

   `./fileserver1.sh`

   This test script first creates the file to be read, which can take 5 minutes or more.

2. Monitor the script output.

   Wait for the screen to update during file creation.

3. After the `Starting with random read` message appears, view information in `esxtop`.
   a. Enter **d** to display the device adapter output.
      Q1. Which adapter has the most disk I/O activity?
   b. Enter **u** to display the individual device output.
      One of the local devices, rather than a remote device, is used for this test.
   c. Enter **v** to display VM output.
4. After 30 seconds of statistics collection, record the values for the Linux01 VM.
   The values can be recorded in the Random Reads/Local Datastore column in the class configuration handout.
   - READS/s
   - WRITES/s
5. In Firefox, select the **Linux01** web console tab.
6. To stop the test script, press **Ctrl+C**.

Task 6: Analyze the Test Results

Your instructor conducts an in-class review and you compare test results from each group.

1. Record the conclusions that you draw from the test data collected in tasks 2 through 5.
   _ _ _ _ _ _ _ _ _ _
2. Keep the **Linux01** web console and the **vSphere Client** open for the next lab.

Lab 18 Monitoring Network Performance

Objective and Tasks

Use the `esxtop` command to monitor network performance:

1. Prepare to Monitor Network Performance
2. Prepare the Client and the Server VMs
3. Measure Network Activity on an ESXi Physical Network Interface
4. Use Traffic Shaping to Simulate Network Congestion
5. Position the Client and the Server on the Same Port Group
6. Restart the Test and Measure Network Activity
7. Stop the Test and Analyze Results
8. Clean Up

Task 1: Prepare to Monitor Network Performance

You use the `esxtop` network statistics screen to monitor network performance.

1. From the student desktop, view the MTPuTTY session to the sa-esxi-04 host.

   MTPuTTY should be logged in to the SA-ESXi-04 host and `esxtop` should be running.
2. If MTPuTTY is not logged in, open a new MTPuTTY session.
   a. In MTPuTTY, open a connection to SA-ESXi-04.
   b. Enter **`esxtop`** at the command prompt.
   c. Set a 10-second screen refresh by entering **`s`** and **`10`**.
3. Enter **`n`** to change to the network statistics screen.

4. Remove unused counters to make the `esxtop` network screen easier to monitor.
   a. Enter **`f`** to display the Current Field Order table.
   b. In the Current Field Order table, enter **`g`** and **`j`** to remove PKTRX/s and PKTTX/s from the `esxtop` display.
   c. Press **ENTER** to return to the network statistics screen.
5. Return to the vSphere Client.

Task 2: Prepare the Client and the Server VMs

You use scripts on the Linux01 and Linux02 VMs to generate network traffic so that network performance can be measured.

The Linux01 VM acts as a client and the Linux02 VM acts as a server. The Linux01 VM is connected to the pg-SA Production port group.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser and click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. Migrate the Linux02 VM to a different VDS.
   a. Select **Menu > Networking.**
   b. In the left pane, expand the **dvs-Lab**.
   c. Right-click **pg-SA-Production** and select **Migrate VMs to Another Network**.

      The Migrate VMs to Another Network wizard appears.
   d. For the Destination network, click **BROWSE..**.
   e. Select **pg-SA-Management** and click **OK**.
   f. Click **NEXT**.
   g. On the Select VMs to migrate page, select the **Linux02** check box and click **NEXT**.
   h. On the Ready to complete page, review settings and click **FINISH**.
   i. In the Recent Tasks pane, monitor the task to completion.

      This migration forces the traffic between the VMs to traverse the physical network.

3. View the IP address of the Linux02 VM.
   a. Select **Menu > Hosts and Clusters**.
   b. Power on the Linux02 VM.

      Wait for the VM to start.
   c. In the left pane, select **Linux02**.
   d. From the **Summary** tab in the right pane, wait a couple of minutes and, after it appears, record the Linux02 IP address. _____

      The Linux02 IP address begins with 172.20.10 (the management network DHCP range).
4. View the IP address of the Linux01 VM.
   a. In the left pane, select **Linux01**.
   b. From the **Summary** tab, record the Linux01 IP address. _____

      The Linux01 IP address begins with 172.20.11 (the production network DHCP range).
5. Start the server on Linux02.
   a. In the left pane, select **Linux02**.
   b. In the right pane, click **Launch Web Console** on the **Summary** tab.
   c. In the Linux02 console window, log in by entering user name **root** and password **VMware1!**.
   d. Navigate to the network scripts folder.

      ```
      cd netperf
      ```
   e. Start the server program.

      ```
      ./netserver
      ```

      The server program runs as a background process.

      Starting netserver at port 12865
      ```
      Starting netserver at hostname 0.0.0.0 port 12865
      ```
   f. Verify that the server program is running.

      ```
      ps -ef | grep netserver
      ```

      The server and grep processes are listed.

      00:00:00 ./netserver
      ```
      00:00:00 grep netserver
      ```

Task 3: Measure Network Activity on an ESXi Physical Network Interface

You measure the network performance of the ESXi host network interface with the Linux01 and Linux02 VMs positioned on different physical network segments across a router.

Requests sent from the Linux01 client enter the physical network through the ESXi network interface vmnic2, which is bound to a dvs-Lab distributed switch uplink. Using the pg-SA-Management port group on the dvs-SA-Datacenter distributed switch, the client requests are routed to the management network where the Linux02 server is.

1. Return to the **Linux01** console tab.
2. Start the client on Linux01.
   a. Navigate to the network scripts folder.

      ```
      cd /root/netperf
      ```

   b. Start the client test script.

      ```
      ./nptest1.sh server_IP_address
      ```

      server_IP_address is the Linux02 IP address that you recorded in task 2.

      The client and server programs must run uninterrupted.
3. Monitor network performance and record your findings.
   a. On the student desktop, return to the MTPuTTY window.
   b. In the `esxtop` output, find the vmnic2 physical network interface.
   c. After 30 seconds of statistics collection, record the values for vmnic2 in the class configuration handout.
      - MbTX/s
      - MbRX/s

Task 4: Use Traffic Shaping to Simulate Network Congestion

You use traffic shaping to control the network speed to simulate congestion.

1. Return to the **vSphere Client** tab.
2. Select **Menu > Networking**.
3. In the left pane, right-click the **pg-SA-Production** port group and select **Edit Settings**.
4. In the Edit Settings dialog box, click **Traffic shaping** on the left.

5. Select **Enabled** from the **Status** drop-down menus for ingress traffic shaping and egress traffic shaping.
6. Configure the ingress and egress traffic shaping.

Option	Action
Average bandwidth (kbit/s)	Enter **`10000`**.
Peak bandwidth (kbits/s)	Enter **`10000`**.
Burst size (KB)	Enter **`10000`**.

7. Verify that you configured both ingress and egress traffic shaping and click **OK**.
8. Monitor network performance and record your findings.
   a. Change to the MTPuTTY window.
   b. In the `esxtop` output, find the vmnic2 physical interface item.
   c. After 30 seconds of statistics collection, record the values for vmnic2 in the vmnic2 10 Mb/s column in the class configuration handout.
      - MbTX/s
      - MbRX/s
9. Disable the ingress and egress traffic shaping.
   a. Return to the **vSphere Client** tab.
   b. In the left pane, right-click **pg-SA-Production** and select **Edit Settings**.
   c. Click **Traffic shaping**.
   d. For both ingress and egress traffic shaping, select **Disabled** from each **Status** drop-down menu.
   e. Click **OK**.

Task 5: Position the Client and the Server on the Same Port Group

You migrate the Linux02 VM back to the pg-SA-Production port group to show that VMs communicating on the same ESXi host and virtual switch port group can communicate at a faster rate than the rate dictated by the physical network hardware.

1. Stop the network client.
   a. Return to the **Linux01** console tab.

b. In the Linux01 console, stop the test script by pressing Ctrl+C.

2. Stop the network server.

   a. Click the **Linux02** console tab.

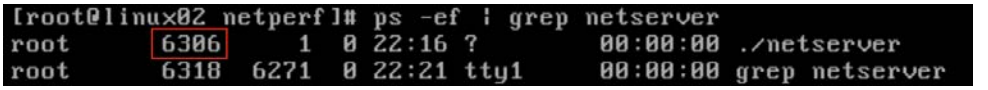
   b. In the Linux02 console, end the server program.

      `ps -ef |` grep `netserver`

      `kill` *<process_id>*

      In the `kill` command, `process_id` is the netserver process ID as reported by the `ps` command.

      In the example `ps` output, the netserver process ID is 6306.



3. Migrate the Linux02 VM to the VDS dvs-Lab.

   a. Return to the **vSphere Client** tab.

   b. In the left pane, expand **dvs-SA-Datacenter**, right-click **pg-SA-Management**, and select **Migrate VMs to Another Network**.

   c. For the Destination network, click **BROWSE..**.

   d. Select **pg-SA-Production** and click **OK**.

   e. Click **NEXT**.

   f. On the Select VMs to migrate page, select **Linux02** and click **NEXT**.

   g. On the Ready to complete page, review settings and click **FINISH**.

   h. In the Recent Tasks pane, monitor the task to completion.

4. Restart the network service and verify that the IP address is within the production network DHCP range.

   a. Select the **Linux02** web console tab.

   b. In the terminal window, restart the network service.

      `service network re`start

      The network service might take up to a minute to restart and acquire a new DHCP address.

   c. Verify that a new DHCP-assigned address was acquired.

      `ifconfig`

d. In the `ifconfig` command output, verify that the IP address begins with 172.20.11 (the production network DHCP range).

e. Record the postmigration Linux02 IP address. _____

Task 6: Restart the Test and Measure Network Activity

You measure network activity when the client and the server communicate across a virtual network contained in a single ESXi host and port group.

1. In the Linux02 console window, run the server program.

   ```
   ./netserver
   ```

2. Return to the **Linux01** console tab.

3. Start the client script.

   ```
   ./nptest1.sh server_IP_address
   ```

   server_IP_address is the postmigration Linux02 IP address that you recorded in task 5.

4. Monitor network activity and record your findings.

   a. Return to the MTPuTTY window.

   b. In the `esxtop` output, find the vmnic2 row and verify that the traffic is no longer traversing the physical interface.

   c. Find the Linux01.eth0 row.

   d. After 30 seconds of statistics collection, record the values for the Linux01.eth0 interface in the class configuration handout.

      - MbTX/s
      - MbRX/s

Task 7: Stop the Test and Analyze Results

You use the data samples recorded earlier to determine if the simulated congestion affected the network performance and to determine the fastest network configuration.

1. Stop the test.
   a. Return to the **Linux01** console tab.
   b. In the Linux01 console, press **Ctrl+C** to stop the client script.
   c. Return to the **Linux02** console tab.
   d. In the Linux02 console, stop the server process to end the server program.

      ps -ef | grep netserver

      kill *process_id*

      process_id is the `netserver` process ID that appears in the `ps` command output.
2. Review the sample values that you recorded in task 6.

   Q1. Do you see an obvious difference in network throughput for each test?

   Q2. Which test resulted in the fastest throughput (highest values)?

   Q3. Why was this test the fastest?

Task 8: Clean Up

You end the `esxtop` program and you close the **Linux01** and **Linux02** console tabs.

1. In MTPuTTY, enter **q** to end `esxtop`.
2. Close the MTPuTTY session.
3. Close the **Linux01** and **Linux02** console tabs.
4. Using the vSphere Client, power off VMs Linux01 and Linux02.

Answer Key

Lab 6 Creating vSAN Storage Policies

Lab 7 Working with Certificates

A1. Under Issuer Information, the Issuer Name field contains CA, which indicates that VMware CA issued the certificate.

Lab 12 Using Host Profiles

Q1. How do the results of the compliance check differ from the compliance check performed in task 6?

A1. The Date and Time configuration did not match. If the category was previously reported, a new issue is added relating to the uplink reconfiguration.

Q2. In the new category Virtual Network Setting, does the specific issue reported relate to the configuration change made in task 7?

A2. Yes. The uplink is not connected to the expected physical NIC on VDS dvs-Lab.

Q3. Will the host need to be put in maintenance mode?

A3. Yes.

Lab 13 Creating Content Libraries

Q1. How much storage space is being consumed in each library?

This value can be found under the Storage Used column on the Content Libraries list page.

A1. Approximately 2.5 GB in publisher library SA-Local-Library, approximately 0 B in subscriber library SB-Subscribed-Library

Q2. How was the amount of storage used not the same between the libraries?

The local (publisher) and subscriber content libraries should have the same content.

A2. The subscriber content library gets its metadata from the local content library. The storage used is only updated when a deployment is attempted from the subscriber library, which forces the download of the VM template from the local content library. The **when needed** configuration was applied to save disk space on the subscriber library side.

Q1. How many VM templates now appear in the SB-Subscribed-Library content library?

A1. Two. SampleVM under OVF & OVA Templates and Photon-01-Library under the VM Templates.

Lab 14 Managing Resource Pools

Q1. What is the number of shares for this RP-Test (Low) resource pool?

A1. 2,000.

Q2. What is the number of shares for this RP-Production (High) resource pool?

A2. 8,000.

Q3. What is the difference in performance between the two virtual machines?

A3. The RP-Test resource pool and the virtual machine in it have only one-fourth of the CPU shares that the RP-Production resource pool has. Therefore, the virtual machine in the RP-Test resource pool receives only one-fourth of the CPU cycles of the logical CPU to which the virtual machines are pinned.

Lab 16 Monitoring Memory Performance

Q1. Is the consumed host memory greater than the active guest memory?

A1. Answers vary depending on the current workload.

Q1. For Linux01, does the value of MCTLSZ converge with the value of MCTLTGT?

A1. Yes, the values should converge over time.

Q2. For Linux01, does the value of SWCUR converge with the value of SWTGT?

A2. Depending on many factors, the values might converge over time.

Q3. Which VMs do not have the balloon driver installed?

A3. ResourceHog02 and ResourceHog01.

Q4. Which VMs are swapping?

A4. Although all three VMs might be swapping, the levels of swapping on ResourceHog01 and ResourceHog02 will be much larger than the level of swapping on Linux01.

Q5. What are the %SWPWT values for each of the VMs?

A5. ResourceHog01 and ResourceHog02 should experience high %SWPWT values because their memory is being swapped out and they must wait whenever those pages are accessed. Linux01 should experience low %SWPWT values, possibly zero.

Q6. What is the memory state: high, clear, soft, hard, or low?

A6. Answers vary.

Q7. Has the performance of the test script degraded?

A7. Answers vary.

Lab 17 Monitoring Storage Performance